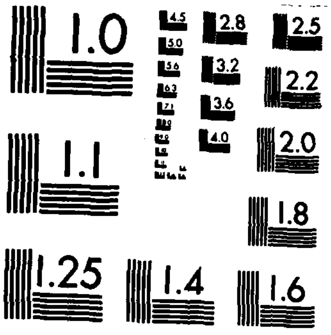
AD-A154 677 SECURE DIGITAL VOICE COMMUNICATIONS IN THE DEFENSE DATA 1/2
NETWORK (DDN)(U) COMPUTER SCIENCES CORP FALLS CHURCH VA
M BERNET ET AL. 15 MAR 85 DCA100-84-C-0030

UNCLASSIFIED F/G 17/2 NL



MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

REPRODUCED AT GOVERNMENT EXPENSE

SECURE DIGITAL VOICE COMMUNICATIONS IN THE DEFENSE DATA NETWORK (DDN)

AD-A154 677

Prepared for
THE DEFENSE COMMUNICATIONS ENGINEERING CENTER

Under
CONTRACT NO. DCA 100-84-C-0030
TASK ORDER 4-84

MARCH 1985

DTIC
ELECTE
JUN 5 1985
S D
A

COMPUTER SCIENCES CORPORATION

6565 Arlington Boulevard
Falls Church, Virginia 22046

Major Offices and Facilities Throughout the World

This document has been approved for public release and sale; its distribution is unlimited.

DTIC FILE COPY

85 05 01 034

REPRODUCED AT GOVERNMENT EXPENSE

1201

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b. RESTRICTIVE MARKINGS None
2a. SECURITY CLASSIFICATION AUTHORITY Not Applicable (NA)	3. DISTRIBUTION/AVAILABILITY OF REPORT Unlimited
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE NA	
4. PERFORMING ORGANIZATION REPORT NUMBER(S) None	5. MONITORING ORGANIZATION REPORT NUMBER(S) None
6a. NAME OF PERFORMING ORGANIZATION Computer Sciences Corporation (CSC) 6b. OFFICE SYMBOL (If applicable)	7a. NAME OF MONITORING ORGANIZATION Defense Communications Engineering Center (DCEC)
6c. ADDRESS (City, State and ZIP Code) 6565 Arlington Boulevard Falls Church, VA 22046	7b. ADDRESS (City, State and ZIP Code) 1800 Wiehle Avenue Reston, Virginia 22090
8a. NAME OF FUNDING/SPONSORING ORGANIZATION Defense Communications Agency (DCA) 8b. OFFICE SYMBOL (If applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER Contract #DCA100-84-C-0030
8c. ADDRESS (City, State and ZIP Code) 8th & South Courthouse Road Arlington, Virginia 22204	10. SOURCE OF FUNDING NOS.

PROGRAM ELEMENT NO.	PROJECT NO.	TASK NO.	WORK UNIT NO.
		4-84	

11. TITLE (Include Security Classification) Secure Digital Voice Communications in the Defense Data Network (DDN) (U)

12. PERSONAL AUTHOR(S)
M. Bernet, D. Gan, C. Oesterreicher

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT (Yr., Mo., Day)	15. PAGE COUNT
Final	FROM Mar 84 TO Mar 85	1985/3/15	138

16. SUPPLEMENTARY NOTATION
None

17. COSATI CODES		
FIELD	GROUP	SUB. GR.

18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
Secure Voice, DDN, Secure Terminal Units (STU), STU-II, STU-IIM, DoD Protocols, Terminal Access Controller (TAC), IPLI, Voice Interface Unit (VIU), Stream Agents (ST), WWDSA

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

This final report has investigated and validated one of the fourteen key features of the future, all-digital Worldwide Digital Systems Architecture (WWDSA), namely "the enhanced 2.4 Kbps secure voice survivability through the use of packetized voice and the interconnection between the voice (DSN) and data (DDN) networks." Key funding of the report is that using the three-phase implementation plan in the report, Secure Voice, as provided by the STU-IIs, can be implemented in the DDN in the late 1980s time-frame with no technical and minimum schedule risk. VIUs are proposed to interconnect, the family of secure voice terminals, called STU-IIs, to the DDN. VIUs contain modem, signalling and supervision (S/S), and processor modules and are supported by the implementation model of the protocol architecture that (with the TAC as processor module) was proposed in the report. An optimum system-level architecture employing the VIUs and the proposed in the implementation plan based on an extensive evaluation.

Keywords include:

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT UNCLASSIFIED/UNLIMITED □ SAME AS RPT. ☒ DTIC USERS □	21. ABSTRACT SECURITY CLASSIFICATION Unclassified

22a. NAME OF RESPONSIBLE INDIVIDUAL	22b. TELEPHONE NUMBER (Include Area Code)	22c. OFFICE SYMBOL
J. O'Neill	(703) 437-2102	DCEC Code R640

EDITION OF 1 JAN 73 IS OBSOLETE.

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

A154 677

SECURE DIGITAL VOICE COMMUNICATIONS IN THE DEFENSE DATA NETWORK (DDN)

Prepared for
THE DEFENSE COMMUNICATIONS ENGINEERING CENTER

Under
CONTRACT NO. DCA 100-84-C-0030
TASK ORDER 4-84

MARCH 1985

COMPUTER SCIENCES CORPORATION

6565 Arlington Boulevard

Falls Church, Virginia 22046

Major Offices and Facilities Throughout the World

TABLE OF CONTENTS

TABLE OF CONTENTS (Cont'd)

Accession For

NTIS GRA&I ☒

DTIC TAB □

Unannounced □

Justification

By

Distribution/

Availability Codes

Dist | Avail and/or Special

A-1

COPY INSPECTED

LIST OF ILLUSTRATIONS

GLOSSARY

ACK	- Acknowledgement
ARPANET	- Advanced Research Project Agency Network
BBN	- Bolt, Beranek, and Newmann
bps	- bits per second
BER	- Bit Error Rate
CINC	- Commander-in-Chief
CS	- Circuit Switched
CSC	- Computer Sciences Corporation
DCA	- Defense Communications Agency
DCE	- Data Circuit-terminating Equipment
DCEC	- Defense Communications Engineering Center
DDN	- Defense Data Network
DG	- Datagram
DIA	- Defense Intelligence Agency
DNA	- Defense Nuclear Agency
DoD	- Department of Defense
DTE	- Data Terminal Equipment
DTMF	- Dual Tone Multifrequency
FEMA	- Federal Emergency Management Agency
FTP	- File Transfer Protocol
HDLC	- High-level Data-link Control
HEMP	- High Altitude Electromagnetic Pulse
HFEP	- Host Front End Processor
HW	- Hardware
IMP	- Interface Message Processor
IP	- Internet Protocol
IPLI	- Internet Private Line Interface
KDC	- Key Distribution Center
KW	- Kilowords
MINET	- Military Information Network
mini-TAC	- Mini-Terminal Access Controller
MILDEP	- Military Departments
MIPs	- Millions of Instructions Per Second
ms	- milliseconds
NAC	- Network Access Controller
NB	- Narrowband
NSA	- National Security Agency
NVP	- Network Voice Protocol
NVT	- Network Virtual Terminal

GLOSSARY

PBX	- Private Branch Exchange
PP	- Protocol Processor
PS	- Packet Switching
PVC	- Permanent Virtual Circuit
RAM	- Random Access Memory
SAD	- Speech Activity Detection
SMTP	- Simplified Mail Transfer Protocol
S/S	- Signaling and Supervision
STD	- Standard
STU	- Secure Terminal Unit
ST	- Stream Protocol
SW	- Software
TAC	- Terminal Access Controller
TCP	- Transmission Control Protocol
TEP	- Terminal Emulation Processor
VC	- Virtual Circuit
VDR	- Voice Digitization Rate
VIU	- Voice Interface Unit
WIN	- WWMCCS Information Network
WWMCCS	- Worldwide Military Command and Control System

EXECUTIVE SUMMARY

ES.1 BACKGROUND, PURPOSE, AND SCOPE

One of the fourteen key features of the future, all-digital Department of Defense (DoD) Worldwide Digital Systems Architecture (WWDSA) is "the enhanced 2.4 kilobits-per-second (Kbps) secure voice survivability through the use of packetized voice and the interconnection between the voice and data networks" [Reference (1)]. The secure voice will be provided by a family of secure voice terminals known a Secure Terminal Units (STU); STU-II, STU-IIM, and their enhancements. Defense Switched Network (DSN) and Defense Data Network (DDN) are planned to be the respective future voice and data networks.

The Defense Communications Agency (DCA) has tasked Computer Sciences Corporation (CSC) to validate this key feature of the WWDSA and to make a recommendation to the Government regarding the value of its implementation.

The following major considerations were used in developing the system-level architectures for incorporating the recommended capability in the DDN.

1. DDN system-level architecture of the near-term (late 1980s) time-frame (or DDN I architecture) was used in the digital packet voice and data integration process, since near-term implementation is the immediate goal of this task effort. This will mean the possible use of security architectures involving Internet Private Line Interface (IPLI) devices for end-to-end security.

2. Point-to-point voice connections, rather than conference (network) type voice connections, were considered for near-term implementation. The idea here is to address the basic issue of adding a secure packet voice capability in the DDN without getting into additional complexities introduced by conferencing.

3. Integration of secure digital voice and data was not explictly addressed in our investigation, since speech activity detection (SAD), which is required for such an integration, is not possible without modification and recertification of the STU-IIs operating in the secure mode.

4. Existing, experimental, or near-term technology in hardware (HW) and the DoD protocols were employed to minimize the additional delta (Δ) cost required to implement secure digital voice capability in the DDN I.

ES.2 SUMMARY OF RESULTS OBTAINED

Major results obtained during the task investigation are summarized in the following paragraphs.

Results Obtained From the Analysis

Packet voice (utilizing voice from the STU-IIs) imposes the following key additional requirements on the system-level architectures:

1. Support for STU-II call initiation and termination

2. Establishment of calling to called STU-II connection. This is always accomplished in the clear

3. Mechanisms within and outside the DDN I to enable near real-time speech delivery (low delay and variance of interarrival time between successive voice packets in a talkspurt)

4. Mechanisms to support:

   a. Digitization of voice from the STU-IIs
   b. Packetization of digital voice
   c. Voice frames assembly into voice packets on the calling STU-II side and voice packet disassembly into voice frames on the called STU-II side

5. Buffers on the called STU-II side to support speech reconstitution function in the STU-IIs.

Security imposes additional requirements on the end-to-end security architectures to be used and on maintaining cyptosynchonization of the calling and called STU-IIs when the STU-IIs are operated in a secure (NET) mode.

These additional requirements were realized by proposing the use of state-of-the-art techniques in the software of the DDN I packet-switched (PS) nodes and gateways and in the hardware and software of the interfaces, called Voice Interface Units (VIU). VIUs are proposed for connecting the STU-IIs to the DDN I PS nodes. Specifically, the additional requirements will be realized as follows.

1. The VIU will contain three modules; Signaling and Supervision (S/S), Modem, and Processor. The S/S Module will support call initiation and termination by providing Central Office functions (dial tone and ringing signals are examples) which are not provided by the DDN I. The Modem Module will allow digitization of voice on the calling STU-II side (for transport in the DDN I) and provide analog voice to the called STU-II. The Processor Module will contain the implementation model of the protocol architecture and necessary control functions for the VIU.

2. The implementation model of the protocol architecture will accomplish call initiation and termination, connection setup [a permanent virtual circuit (PVC) if stream (ST) agents are implemented in the DDN I PS nodes and gateways], near real-time speech delivery (using time stamps and sequence numbers on voice packets and minimizing overhead in them), packetization of digital voice, and voice assembly and disassembly.

3. Buffers to hold voice packets will be provided in the Processor Module of the VIU.

4. The following security architectures will be used for obtaining the end-to-end security:

   a. Clear voice from the STU-IIs with the IPLIs
   b. Secure voice from the STU-IIs (NET mode) without the IPLIs
   c. Secure voice from the STU-IIs (NET mode) with the IPLIs yielding double encryption.

5. To maintain cryptosynchronization, when secure voice from the STU-IIs (NET mode) is used, bit count integrity will be enforced by the protocol on the called STU-II side.

Alternative System Level Architectures

The alternative system-level architectures to incorporate the STU-IIs in the DDN I can be grouped into two major catagories of interfacing options; interfaces using ST agents in the DDN I PS nodes and gateways or interfaces without using ST agents. In the former option, the DDN I backbone is employed as a PS network; in the latter option, as a circuit-switched (CS) emulator. As shown in Illustration ES-1, additional major subcatagories result from:

1. The end-to-end security architecture employed (NET mode of STU-IIs and/or IPLIs)

2. The type of processor used in the Processor Module of the VIU [DDN I supplied Terminal Access Controller (TAC) and/or external processor(s)]

3. Direct connection of the STU-IIs versus connection of the STU-IIs when they are behind a Private Branch Exchange (PBX). The S/S-I Module is needed for Direct Connection, while the S/S-II Module is used for Behind-the-PBX connection.

All subcatagories (a total of 48) of system-level architectures are supported by the implementation model of the protocol architecture.

No.	Top Level Requirement	Lower Level Requirements			
1	Worldwide Survivability	1.	Invulverability*	1.	Physical Threats
				2.	Electronic Threats
				3.	Nuclear Threats
		2.	Survivability Measures	1.	Call Completion Rate (Voice) or
				2.	Probability of Correct Message Delivery (Data)
		3.	Restorability	1.	Network Capacity
2	Security	1.	Passive Intercept Resistance	1.	At Nodes
				2.	On Links
		2.	Spoofing Resistance	1.	False/Altered Messages
				2.	Denial of Service
		3.	Traffic Analysis	1.	From/To Distribution
				2.	Link Volumes
		4.	Key Protection	1.	Storage Method
				2.	Loading Method
				3.	Distribution Method
		5.	Unauthorized Access	1.	Physical (Intruder)
				2.	Logical (Authorized User)
		6.	Certification*		
3	Performance	1.	Timeliness	1.	Call Setup Time (Voice) or
				2.	Speed of Service (Data and Packetized Voice)
		2.	Quality	1.	Intelligibility and Naturalness (Voice) or
				2.	Bit Error Rate (Data)
4	Responsiveness	1.	Interoperability*		
		2.	Adaptability*		
		3.	Ease of Upgrade*		

* Primarily "qualitative" requirements

Illustration 2-1. Military Network Requirements Breakdown

3. Performance - The ability of the network to provide the timeliness and quality of services required in military network users' missions/applications.

4. Responsiveness - The ability of the network to operate with other networks (interoperability), its ease of upgrade (with future technological improvements), and adaptability.

These top level requirements are further subdivided into lower levels to arrive at "quantitative" requirements so that some "score" or "judgement" can be associated with them to permit evaluation of the alternative architectures (see Paragraph 2.4). This subdivision is detailed in Appendix A and summarized in Illustration 2-1.

The DDN goal architecture will satisfy the military network requirements listed in the Illustration associated with data users or applications. Integration of secure voice users in the DDN as a backup mode of operation is an added goal which is being *investigated in this report.*

2.1.2 Additional Requirements Imposed on a PS Network by Packet Voice in Point-to-Point Connections

Major requirements to be supported by a PS network to implement point-to-point connections for packet voice are summarized in the following.

1. Setting up a Circuit for a Call - The network must support implementations which perform the following functions:

   a. Call initiation and termination. It involves signaling and supervision (S/S) for handling dialing [Dial Pulse and Dual Tone Multi-Frequency (DTMF) are examples] ringing, and ON-HOOK and OFF-HOOK states.

SECTION 2 - ANALYSIS

2.1 REQUIREMENTS DEFINITION

The Requirements Definition provides "qualitative" requirements for implementing a secure packet speech capability in the DDN employing the STU-II family of secure voice terminals. The emphasis is on "qualitative" rather than "quantitative" requirements since the immediate goal is to define (higher) system-level alternative architectures for implementation when sufficient details will not be worked out using modeling and simulation or test-beds to permit quantitative evaluation. General military network requirements are defined first followed by other (unique) requirements associated with the implementation of packet voice (and users of this capability) and the STU-II family of secure voice terminals in a PS network.

2.1.1 Military Network Requirements

The military networks such as the DDN have fundamental requirements for survivable, secure, reliable and timely, and responsive communications in both normal situations (unstressed environment) and abnormal situations (stressed environments) resulting from crisis or enemy threats [primarily physical, electronic (jamming is an example), and nuclear threats]. The military network requirements can be divided, for the purpose of this task effort, into the following "qualitative" categories.

1. Survivability - The ability of the network to continue its operation in stressed environments.

2. Security - The ability of the network to protect information entrusted to it and prevent security violations resulting in unauthorized disclosure, modification, or destruction, or denial of service.

corresponding to the Evaluation and Implementation work-elements. Necessary details on military network requirements, DDN I baseline architecture, and the implementation model of the protocol architecture to support secure digital voice in the DDN I are respectively presented in Appendices A, B, and C. The Appendices pull together information scattered over many documents into one place in order for the reader of this report to have a good understanding of the material presented in the main body of this report. A classified appendix, Appendix D, in a separate document, provides the necessary information on the STU-II family and scenarios (call initiation/termination, connection setup, and secure digital voice transmission).

emphasis. The Evaluation of Alternatives is the assessment of the alternative architectures develope. under the Definition of Alternative System-Level Architectures work-element, to provide recommendations regarding the feasibility of implementing secure packet voice capability in the DDN I.

The Implementation Plan work-element focuses on how to implement the recommendations for a subsequent proof of the techniques involved in the VIUs. This will encompass hardware acquisition, software development, and transition and scheduling, including future modeling and simulation efforts and test-bed implementation.

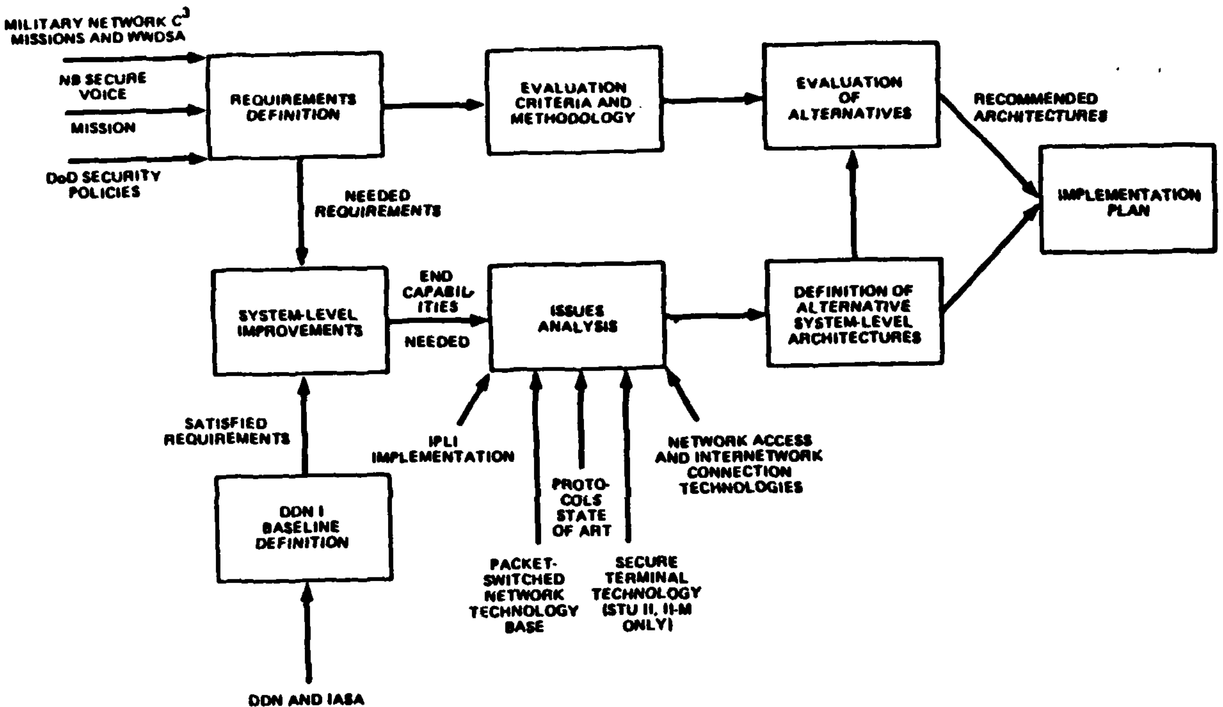
1.4 ORGANIZATION

This Final Technical Report provides a detailed status of the work accomplished during the task investigation. Section Two, Analysis, describes the completion of work under the Requirements Definition, DDN I Baseline Definition, System-Level Improvements and Issues Analysis, and Evaluation Criteria and Methodolgy work-elements. Alternative system-level architectures (to implement a secure packet voice capability in the DDN as a backup mode employing the STU-II family of secure voice terminals) are described in Section Three. Two generic ways of interfacing the family are presented: (1) interfaces using special ST agents in the PS nodes and gateways of the DDN I, together with supporting protocols in the interfaces, and (2) interfaces without ST agents, which essentially employ the DDN I as a circuit-switched (CS) emulator.

Additional major interfacing subcatagories result from the end-to-end security architecture used (NET mode of STU-IIs and/or IPLI), the type of processor used in the VIUs, and direct connection of STU-IIs to VIUs versus connection when the STU-IIs are behind a Private Branch Exchange (PBX). Section Four contains evaluations, recommendations, and implementation details requirements resulting from the employment of the specified STU-II family of secure voice terminals, including the DoD security policy and the use of PS technology to integrate digital voice and data, to generate "needed requirements" for secure packet voice implementation in the DDN. The DDN I Baseline (Architecture) Definition work-element defines the system-level capabilities of the DDN I, which are assessed in the System-Level Improvements work-element to determine which of the "needed requirements" are satisfied by the baseline. This results in the additional "end capabilities" needed to incorporate the secure packet voice capability in the DDN. In the Issues Analysis, the "end capabilities" needed are analyzed in the light of the state-of-the-art technologies in PS networking, protocols, end-to-end security architectures, and network access and internetwork connection to arrive at the techniques that will be used to develop the alternative system-level architectures.

These architectures are defined under the Definition of System-Level Architectures work-element. Essentially, they describe the interface devices [to include HW, software (SW), needed protocols, and control functions] and any required modifications in the DDN I, which are required to connect the STU-II family of secure voice terminals to the DDN. These interface devices, called Voice Interface Units (VIU) henceforth, is the focus of this effort.

Evaluation criteria, which are derived primarily from the Requirements Definition (in consultation with the Government Task Officer), are used in the methodology defined under Evaluation Criteria and Methodology work-element, for comparative evaluation of the alternative system-level architectures. Evaluation criteria exert strong influence on these alternative architectures, by indicating those end capabilities that deserve


MILITARY NETWORK C³ MISSIONS AND WWDSA
NB SECURE VOICE
MISSION
DoD SECURITY POLICIES
REQUIREMENTS DEFINITION
EVALUATION CRITERIA AND METHODOLOGY
EVALUATION OF ALTERNATIVES
RECOMMENDED ARCHITECTURES
IMPLEMENTATION PLAN
NEEDED REQUIREMENTS
SYSTEM-LEVEL IMPROVEMENTS
END CAPABILITIES
NEEDED
ISSUES ANALYSIS
DEFINITION OF ALTERNATIVE SYSTEM-LEVEL ARCHITECTURES
SATISFIED REQUIREMENTS
IPLI IMPLEMENTATION
PROTOCOLS STATE OF ART
NETWORK ACCESS AND INTERNETWORK CONNECTION TECHNOLOGIES
DDN I BASELINE DEFINITION
PACKET-SWITCHED NETWORK TECHNOLOGY BASE
SECURE TERMINAL TECHNOLOGY (STU II, II-M ONLY)
DDN AND IASA DOCUMENTS

TP No. 084-15021-A

Illustration 1-1. Technical Approach to the Task Effort is planned for use in a longer-term (1990s) time-f'ame (for DDN II architecture), involving multi-level security (MLS) and key distribution centers (KDC) for key variable distribution and key management, will be deferred. Any references to DDN will henceforth, unless otherwise stated, imply DDN I.

3. Point-to-point voice connections rather than conference (network) type voice connections will be considered for near-term implementation. The idea here is to address the basic issue of adding a secure packet voice capability in the DDN without getting into additional complexities introduced by conferencing.

4. The integration of secure packet voice and data was not explictly addressed in our investigation since speech activity detection (SAD) is not possible without expensive modifications and recertification of the STU-IIs in the secure mode of STU-II operation.

5. Use of existing, experimental, or near-term technology in HW and protocols for integration of secure digital voice and data communication. The central idea here is to minimize the additional delta (Δ) cost required to implement this capability. Terminal Access controller (TAC) for hardware and and Network Voice Protocol/Stream (NVP/ST) for protocol are examples.

1.3 TECHNICAL APPROACH

Our technical approach to the task effort was organized into eight work elements, as depicted in Illustration 1-1 and summarized below.

The Requirements Definition work-element defines the military requirements necessary to satisfy the C^3 missions of the high priority users [Fixed Commands/Executing Commands (FC/EC) is an example], including the users of NB secure voice, particularly in the stressed environment. It synthesizes other additional

1.2 PURPOSE AND SCOPE

The DCA tasked Computer Sciences Corporation (CSC) to validate this key feature of the WWDSA and to make a recommendation to the Government as to the value of its implementation. The major thrust of the task is to:

1. Research the previous/current packet speech accomplishments
2. Develop techniques for accommodating/integrating secure packet speech in the DDN
3. Define and evaluate the alternative system-level architectures which will provide an end-to-end secure packet speech capability in the DDN. The evaluation is to include a risk assessment.

After an extensive dialogue with the Government Task Officer, and as a result of Government comments received on the Draft Report [Reference (2)], it was mutually agreed that CSC focus its attention on the following considerations in developing the system-level architectures.

1. Secure voice, as provided by the family of secure voice terminals; STU-II, STU-IIM, and their enhancements, will be considered for integration in the DDN. This family employs a DoD standard (STD) LPC-10 algorithm in voice processing that is suitable for operation on 2.4 Kbps narrowband (NB) channels.
2. DDN system-level architecture of the near-term (late 1980s) time-frame (or DDN I architecure) will be used in the integration process, since near-term implementation is the immediate goal of this task effort. This will mean the possible use of security architectures involving Internet Private Line Interface (IPLI) technology to implement end-to-end security. BLACKER technology, which

SECTION 1 - INTRODUCTION

1.1 BACKGROUND

Worldwide Digital Sysem Architecture (WWDSA), documented in Reference (1), provides a common "roadmap" for the evolutionary growth of all DoD digital telecommunications. The primary purpose of developing this goal WWDSA is to assure that the many DoD command, control, and information processing systems are sufficiently interoperable to achieve the needed survivability and endurability.

The WWDSA study was conducted with the aid of a joint working group, whose membership included representations from the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence [ASD (C^3I)]; Office of Joint Chiefs of Staff (OJCS); all Commander-in-Chiefs (CINC); all Military Departments (MILDEP); the Defense Communications Agency (DCA); the TRI-TAC office; and a number of DoD agencies [National Security Agency (NSA), Defense Intelligence Agency (DIA), Defense Nuclear Agency (DNA), and Federal Emergency Management Agency (FEMA) are some examples.] The mode of operation called for the WWDSA architectures to be developed by the Defense Communications Engineering Center (DCEC) on a "strawman" basis, and then to be presented at the working group sessions for comments and information. After many iterations, the working group sessions arrived at eight alternative WWDSA architectures. These were evaluated using an extensive and formal evaluation process, resulting in the selected WWDSA goal architecture.

The selected WWDSA goal architecture can be described by its fourteen key features, which are stated in the executive summary of Reference (1).

One key feature of the WWDSA goal architecture is "the enhanced 2.4 Kbps secure voice survivability through the use of packetized voice and the interconnection between the voice and data networks."

of the Modem and S/S Modules in the VIUs at the calling and called STU-II sites (these modules are assumed non-sharable). Bulk purchasing of these items may reduce the cost per connection.

Transition and scheduling will include modeling and simulation and test-bed (pilot system) implementation (of one calling to called STU-II connection), primarily to validate in the real-world situation the end-to-end performance of secure voice packets employing VIUs (with the TAC as the Processor Module containing the protocol architecture) and special ST agents in the DDN I PS nodes and gateways. Scheduling indicates how the hardware acquisition, software development, modeling and simulation, and test-bed implementation will be conducted in time, using sound system engineering and acquisition processes to realize the desired goal of implementing the secure voice (as provided by the STU-IIs) in the DDN I with minimum risk, both technical and schedule, in the late 1980s time-frame. There is no technical risk involved and a realistic schedule has been worked out.

Conclusions

Finally, we recommend that the Phases one and two of the implementation; which define the functional requirements, A- and B- specifications of the necessary hardware and (protocol) software, and modeling and simulation, be started as soon as possible (certainly no later than October 1985) to implement the secure voice, as provided by the STU-IIs, in the calendar year of 1989. The Phase one and two cost is estimated at roughly $331K. Funding efforts for the Phase three, which immediately follows the Phases one and two of the implementation, must also be initiated.

Recommended Alternative System-Level Architecture

The scores, using the selected weight distribution of the evaluation criteria, indicate that the optimum (highest score) system-level architecture requires special ST agents in the DDN I PS nodes and gateways, employs the NET mode of STU-IIs for end-to-end security with the STU-IIs Behind a PBX, and interfaces the STU-IIs to the DDN I via the VIU containing the TAC. A further sensitivity analysis of the architectures' scores with respect to top level criteria ("Effectiveness" and "Implementation") confirms this for the practical "Effectiveness" weight range of 14-63% (see Paragraph 4.2.2).

Implementation of the Recommended Alternative System-Level Architecture

A three-phase implementation of the recommended architecture has been proposed (see Illustration 4-11). It will involve hardware acquisistion, software development, and transition and scheduling.

The Modem and S/S Modules in the VIU are the additional hardware components required when using the DDN I-supplied TAC as the Processor Module in the VIU.

An implementation model of the protocol architecture will have to be developed in the software and integrated with the existing software in the TACs. The DDN I PS nodes and gateways will have to incorporate ST agents software, requiring software development and integration.

Δ - Cost, which is the cost over and above what the DDN I can provide, of this hardware acquisition and software development, is estimated at roughly $965K (for all three phases, including the test-bed implementation costing of $634K) for incorporating the first calling STU-II to called STU-II connection in the DDN I. Additional connections can be incorporated at the cost of roughly $10K per connection, which is essentially the cost

Evaluation of the Architectures

The evaluation of thᴗ alternative system-level architectures was conducted employing the evaluation criteria and methodology developed during our Analysis.

The evaluation criteria contains "Effectiveness" and "Implementation" as the two top level criteria. These are further subdivided into lower level criteria until some "score" can be associated with them when evaluating the architectures (see Paragraph 2.4.1).

The evaluation methodology developed is similiar to that used in the WWDSA study [Reference (1)]. Using the subdivision of the evaluation criteria as stated in the previous paragraph, weights were associated with the lower level criteria which "discriminate" among the architectures by expressing the relative value of the criteria. These weights add up to a value of 100% at the top level. In our investigation, since "Implementation" (including Δ - cost lower level criteria) is of far more importance than "Effectiveness" (including Performance lower level criteria), their respective selected weights were 80% and 20%.

Starting at the lowest level criteria, evaluation of the architectures was carried out by expressing the performance of an architecture in terms of its raw score in the criteria. These raw scores in various evaluation criιeria were summed up, after multiplying them with the weights of the evaluation criteria, to arrive at a score which was used in the next higher level. This scoring continued to the top level criteria wherein, effectively, the weighted lower level scores were collapsed into a single number that gives the score of the alternative under evaluation. The evaluation, for selected evaluation criteria weight distribution, is shown in Illustration 4-5.

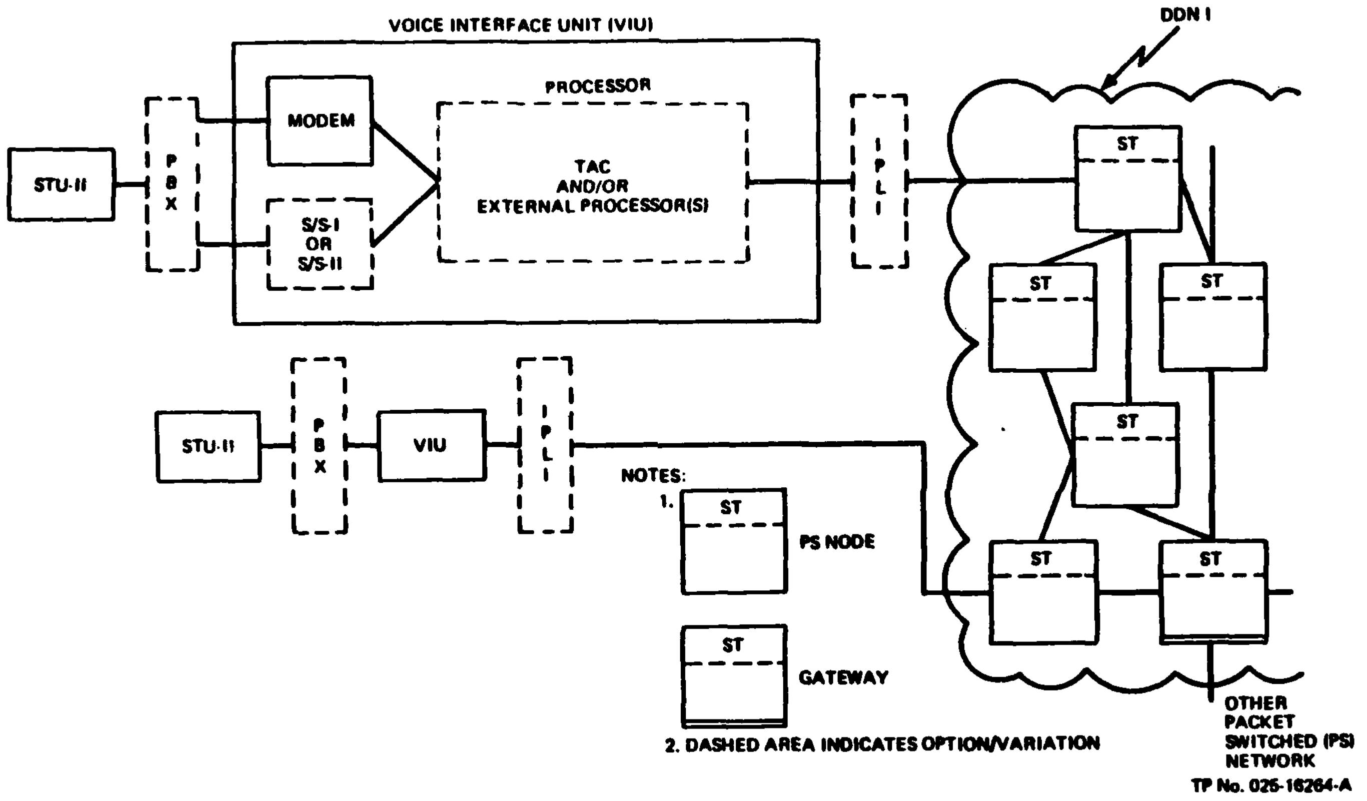

VOICE INTERFACE UNIT (VIU)
PROCESSOR
MODEM
STU-II
P B X
S/S-I OR S/S-II
TAC AND/OR EXTERNAL PROCESSOR(S)
P L I
DDN I
ST
ST
ST
ST
ST
ST
STU-II
P B X
VIU
P L I
NOTES:
1.
ST
PS NODE
ST
GATEWAY
2. DASHED AREA INDICATES OPTION/VARIATION
OTHER PACKET SWITCHED (PS) NETWORK
TP No. 025-16264-A

Illustration ES-1. Possible System-Level Architectures

b. Connection setup

c. Negotiations - Usually for calling and called party to agree on transmission parameters such as data rate and voice encoding scheme. In the backup mode of operation that is considered in this investigation, no such negotiations are required since the data rate is already at the minimum and other negotiable parameters are considered to be agreed upon prior to invoking this mode.

d. Voice packet transport.

2. Near Real-Time Delivery - The network must support implementations which will allow near real-time delivery (low delay and delay dispersion or interarrival time) of packets containing digitized voice (voice packets) from a talkspurt for natural sounding voice at the receiver.

3. Voice Packet Loss - The number of voice packets in a talkspurt lost at the receiver as a result of misrouting or execess delay in the network, must be kept low for minimum degradation of intelligibility.

4. Network Blockage - In a congested (load-limit) situation the network must not block new offered load arising out of voice packets from calls already in progress. Such a blockage would result in gaps in received speech and overall unsatisfactory communication for voice users. New calls may be buffered and allowed in the network when the load falls below a certain threshold.

5. Speech Reconstitution - The network must support implementations which provide for a) buffering of received voice packets in a talkspurt and b)

decision-making algorithms which determine what voice packet to play out next and what to do when no next voice packet is available. Natural sounding voice is the primary goal of these implementations.

6. Statistical Multiplexing of Voice and Data Packets

A PS network provides for statistical multiplexing of data packets usually at its PS nodes. Statistical multiplexing of voice and data packets and supporting algorithms which perform speech activity detection (SAD), when a talkspurt begins and end of talkspurt, is needed only when clear (unencrypted) voice from the STU-II is employed. The required statistical multiplexing function may take place within the PS node of the PS network or outside the network. This investigation does not address this function as a part of system-level architectures to be developed.

2.1.3 Additional Requirements Generated by Features Unique To The STU-II Family of Secure Voice Terminals

In the secure mode of operation, the STU-II family of secure voice terminals provide black (encrypted) analog or black digital voice at their output ports for inte face with the DDN. They can also be operated in a non secure mode that allows clear (unencrypted) calls to be made like ordinary telephone units. Signaling and supervision (S/S) is in the clear (not encrypted) and is also available at the output port (through 4-wire or 2-wire line interfaces) for interface with the DDN. The following additional requirements arise out of the unique way this family operates (see Appendix D for details).

1. Security Related Requirements:

a. In the secure mode of operation, cryptosynchronization must always be maintained between the calling STU-II and the called STU-II after cryptoinitialization. This will mean that the called STU-II must, after cryptoinitiatization, see the same number of bits (bit count integrity) as sent by the calling STU-II. The received bits may contain errors, however.

b. In the Key Distribution Center (KDC) mode of operation, which is not desirable for the backup mode of operation of the investigation (primarily because of additional delays involved in obtaining call variables from the KDCs), the KDC (voice) must be capable of operating and have suitable interfaces with the DDN to allow for call variable transfer.

c. In the NET mode of operation, assignment of call variable to a community of critical users is possible within a specific network.

d. Certification requirement will arise at least in the following three instances:

(1) Attachment and use of a KDC (voice) in the PS DDN, a data network. This may be a violation of some security doctrine if the KDC mode is selected for use in the backup mode of operation to support secure packet voice.

(2) In the secure mode of operation, a potential need for a crypto bypass in the STU-IIs to allow for the SAD. This may involve major modifications in the STU-IIs.

(3) Red/Black separation design if clear voice from the STU-IIs is employed.

2. Performance Related Requirements:

a. Additional delays introduced by the Voice Interface Units (VIU), which interface the STU-II family to the DDN, and the DDN transport must not disrupt cryptosynchronization.

b. Overhead introduced into the packets by protocols (special and standard) incorporated in the VIUs must be minimized to facilitate near real-time delivery of voice packets.

c. The DDN must be able to recognize VIUs, STU-IIs, and KDC (voice), if employed and possible. This means that these must be part of the DDN directory and the VIUs must provide the necessary translation between the directories and numbering plans used by the STU-IIs and the addressing used in the DDN.

3. Implementation Related Requirements:

a. Cost - Primarily the cost of implementing the secure voice capability in the DDN I to satisfy the requirements stated in Paragraphs 2.1.1 and 2.1.2. Protocols in the VIUs, special ST agents in the DDN I PS nodes, and S/S hardware in the VIUs are examples (see Paragraph 2.3).

b. Risk - Basically the technical risk (technology not being available) and schedule risk (implementation date slipping by more than a specified amount from the planned date) associated with implementing the secure voice capability in the DDN I in late 1980s time-frame.

2.2 DDN I BASELINE (ARCHITECTURE) DEFINITION

2.2.1 General

The DDN goal network architecture to satisfy all DoD data network requirements, will evolve in two stages, DDN I and DDN II. The DDN I will evolve from the integration of Worldwide Military Command and Control System (WWMCCS) Information Network (WIN), Advanced Research Project Agency Network (ARPANET), and Military Information Network (MINET) into a common data network and incorporate Internet Private Line Interfaces (IPLI) for end-to-end security. The DDN I is expected to be operational in the late 1980s time-frame which is the basis of the alternative architectures of this task effort. In the post-DDN I time-frame, when BLACKER technology for multilevel security (MLS) and end-to-end security using KDC (Data) becomes available, the DDN I will evolve into DDN II.

The purpose of this DDN I Baseline Definition is to determine which of the "needed" requirements for secure packet voice integration in the DDN are satisfied by the baseline.

The DDN I will include the data network backbone and much of the access lines and access equipment which enable data subscribers to use the backbone. The DDN I baseline features can be described in terms of components used in three general catagories: network backbone, access area, and protocols. The features are described in detail in Appendix B. The DDN I capabilities are examined in Paragraph 2.2.2 to determine what "needed requirements" are satisfied by the DDN I.

2.2.2 DDN I Capabilities

The DDN provides for data transfer between a source host and a destination host; the data subscribers (terminals and hosts) forward the data to source PS node directly or through the access area components [Terminal Access Controller (TAC) is an example] described in Appendix B. The source PS node takes the data usually at High-level Data Link Control (HDLC) Distant Host (HDH) interfaces in message segments and forms packets, or at X.25 interfaces as packets and transmits the packets over the network to a destination PS node. The destination PS node reassembles the packets, if necessary, and delivers them to the destination host. The PS node provides for PS node-to-PS node error free transmission, precedence processing, non-blocking of source host link to highest precedence levels (when resources are not available in it). The last feature can be particularly useful for critical voice calls already in progress which may be assigned the highest precedence.

Analysis of the DDN I features provided in Appendix B reveal that the DDN I can provide network backbone services at network, data link, and physical levels for packet voice transmission. Results of this analysis are summarized in Illustration 2-2 which shows which of the "needed requirements" are satisfied by the DDN I baseline capabilities.

2.3 SYSTEM-LEVEL IMPROVEMENTS AND ISSUES ANALYSIS

2.3.1 System-Level Improvements Needed

System level improvements are the additional end capabilities needed to satisfy all additional requirements introduced by point-to-point connections for packet voice and by a need to interface the STU-II family of secure voice terminals to the DDN I (see Paragraph 2.1 and Illustration 2-2).

Major additional requirements imposed on the DDN I network backbone and architectures for incorporating the STU-IIs in the DDN I are:

1. Measures on survivability and performance for packet voice
2. The security architecture which will make use of the STU-II NET mode and/or DDN I provided IPLIs (in conjunction with clear voice from STU-IIs) for end-to-end security

Needed Requirement	Capability in DDN I Backbone (Network, Data Link, and Physical Levels)	Requirement Satisfied, Yes or No & (Comments)
1. Invulnerability	Provided by highly distributed network with adequate built-in features (line redundancy, dispersion, hardening and HEMP protection, reconstitution, and pre-planned homing) to survive the JCS postulated threats	Yes (With qualification as shown in Illustration 2-3)
2. Survivability		
3. Restorability		
4. Security	Provided through features including link-encryption (using KG-84s), end-to-end encryption (using IPLIs), application of physical and procedural security measures, and monitoring center (MC)- switch communications security	Yes (with qualification as shown in Illustration 2-3)
5. Performance	Optimized for data users employing features such as dual-homing, error detection and correction (PS node-to-PS node and end-to-end), and precedence/ preemption	Yes (with qualification as shown in Illustration 2-3)
6. Interoperability	Planned for interoperability with DoD data networks such as SACDIN	No (no provision currently for supporting secure, packet voice in it)
7. Call initiation and termination	None	No
8. Connection setup	Yes (Virtual Circuits)	Yes
9. Negotiations	None	No

Illustration 2-2. Needed Requirements Versus DDN I Backbone Capabilities (Page 1 of 2)

Needed Requirement		Capability in DDN I Backbone (Network, Data Link, and Physical Levels)	Requirement Satisfied, Yes or No & (Comments)
10.	Packet voice	None	No
11.	Buffers for packet voice	None	No
12.	Near real-time speech delivery	None	No
13.	SAD	None	No
14.	Statistical multiplexing of voice and data packets	Possible	No
15.	Voice packets assembly and disassembly	Possible	No
16.	Speech reconstitution	Possible	No
17.	KDC (voice) and STU-II addressing	None	No
18.	DDN access to STU-IIs	None	No
19.	Crypto-synchronization for STU-IIs	None	No

Illustration 2-2. Needed Requirements Versus DDN I Backbone Capabilities (Page 2 of 2)

3. A mechanism which will allow physical and logical connection of the STU-IIs to the DDN I for interoperability

4. Mechanisms to support STU-II call initiation and termination

5. Capability to support a connection setup (including negotiations, if used) between the calling and called STU-IIs

6. Mechanisms, within and outside the DDN I, which will enable a near real-time speech delivery

7. Mechanisms which will support:

   a. Packetization of voice in the talkspurts

   b. Buffers on the calling STU-II side to allow for DDN I network delay and on the called STU-II side in support of speech reconstitution function in the STU-IIs

   c. Voice packet assembly on the calling STU-II side and voice packet disassembly on the called STU-II side.

8. When clear voice from the STU-IIs is employed, a SAD function

9. Mechanism to allow for statistical multiplexing of voice and data packets when the SAD function is feasible (see item 8)

10. Capability for addressing KDC (voice), if used, and the STU-IIs in the DDN I

11. Protocols which will support STU-IIs access to the DDN I

12. When black (or encrypted) voice from STU-IIs is employed (as in the case of NET mode), mechanisms to maintain cryptosynchronization between the calling and called STU-IIs.

In order to meet these additional requirements some sort of interface, called Voice Interface Unit (VIU) henceforth, is required to incorporate the STU-IIs in the DDN I whether they are to be connected directly or via a PBX. There is a need to define the hardware (HW) and software (SW) architecture of the VIU whose functions and interfaces facilitate:

a. Call initiation and termination

b. Connection setup and negotiations

c. Voice digitization (of black or clear voice from STU-IIs) and packetization (voice packets)

d. Voice packet transport

e. SAD, if feasible

f. Sufficient buffers at the calling and called STU-IIs sites

g. Signaling/supervision HW to generate appropriate signals (dial tones and ringing are two examples)

h. Binary digital code translation to provide suitable control signals for signaling/supervision HW and to convert dialed digits to the DDN addresses and vice versa

i. Proper input port to output port connections in the Behind-the-PBX setup

j. Protocols in support of:

   (1) Near real-time speech delivery
   (2) SAD, if feasible
   (3) Statistical multiplexing of voice and data packets, if employed
   (4) Voice packet assembly (from voice frames of the LPC-10 in a talkspurt) and disassembly (for reconstitution of voice frames into a talkspurt)

(5) Speech reconstitution algorithms (if necessary) for voice playout to support STU-II speech reconstitution function

(6) KDC (voice) (if employed); VIU; and STU-II addressing in the DDN

(7) Binary digital codes used for signaling/supervision and STU-II control messages such as GO SECURE and ANSWER

(8) DDN access. Standardized protocols (X.25 and/or ARPANET technology based) will be utilized to the extent possible to interface the VIU to the DDN PS node.

k. Mechanisms to maintain cryptosynchronization.

2.3.2 Issues Analysis

In issues analysis, techniques in the state-of-the-art technologies including PS networking, DoD and commercial protocol activities, DDN access and internetwork connection, and generic PBX functionality, were analyzed to select those techniques which will implement the end capabilities needed (see the preceding Paragraph). The selected techniques are described in the following.

1. Secure voice at 2.4 Kbps as provided by the STU-IIs has been used. Secure voice is provided by STU-IIs in its secure mode of operation employing either a NET mode or a KDC (voice) mode. Primarily because of the undesirable delays introduced to obtain call variables from KDC (voice) and cost penalty resulting from the need to interface the KDC (voice) to the DDN, it was decided to defer the use of the KDC mode. The STU-IIs can also be operated as ordinary telephone units to provide clear (unencrypted) voice. IPLI then can be used to provide end-to-end security. Therefore, the following security architectures were selected for use in obtaining the end-to-end security:

a. Clear voice from STU-IIs with IPLIs

b. Secure voice from STU-IIs (NET mode) without IPLIs

c. Secure voice from STU-IIs (NET mode) with IPLIs yielding double encryption.

2. The DDN provides a PS capability at its backbone nodes. Additionally the DDN, under light load conditions, provides a physically fixed permanent virtual circuit (PVC) for packet transport, in effect acting as a CS emulator [Reference (23)]. To make use of these possible capabilities within the DDN I, it was decided to consider the following two options for interfacing the STU-IIs to the DDN:

   a. Use of the DDN I as a PS network

   b. Use of the DDN I as a CS emulator.

3. Protocols have been successfully developed and experimented with to support near real-time speech delivery and to implement a packet voice capability in a PS network [see References (12), (13), (22)]. These protocols can be used, with some modifications/enhancements, in interface options of item 2 above. Additional complications are introduced in our investigation as a result of a specific family (as against a generic capability) of secure voice terminals used and security, resulting in the consequent need, respectively for custom design of and security feature in the interface options within the VIUs. Additionally, the protocols to be used in the VIUs must employ the state-of-the art technology in accessing the PS DDN, implying the use of planned X.25 DDN access protocols [Reference (6)]. The implementation model of the protocol architecture has been proposed in our investigation to take into account the stated major factors. It is based on the proven protocols for packet voice (NVP and supporting ST), for packet transport in CATENET environment (IP), and for PS network access (X.25). For in-depth details, see Appendix C.

The proposed architecture will be implemented in software for reasons including standardization, flexibility, availability of a processor in the VIU, and ease of future integration with packet data protcols (TCP in partcular). The major modifications/enhancements and capabilities of the proposed protocol architecture are summarized in the following. Primarily it consists of two major functions, Data Voice Server (DVS) and Data Voice Transfer (DVT) which will be implemented in the Voice Interface Processor (VIP) of the VIU.

The DVS consists of three higher level protocols: Voice Application Protocol (VAP), Voice Presentation Protocol (VPP), and Voice Session Protocol (VSP). It interfaces to the STU-IIs and handles the STU-II messages (voice and control) and signaling and supervision (S/S). Primarily it is based on the NVP and supports call initiation and termination, logical connection setup and negotiations, voice packet assembly and disassembly, buffers and their management, cryptsynchronization, and binary digital code translation.

The other function, DVT, consists of lower level protocols: special voice protocol (NVP/ST) based primarily on the ST with modifications, standard IP, and (planned) DDN X.25. It interfaces the DVS on the STU-IIs side and the DDN PS node on the network side. It enables voice packet transport using the DDN STU-II address (employing the PVC connection setup by the NVP/ST using the DDN STU-II address - a fixed physical path when ST agents are implemented in the DDN PS nodes and gateways - and the standard IP datagram service) and voice packet access to the DDN employing the X.25. The DVS and DVT, as stated earlier, will reside in the VIP [TAC and/or external processor(s) used in the VIU].

4. A signaling and supervision (S/S) hardware is required to provide the capabilities usually available in the Central Office on the trunk side of a telephone unit since they are not provided by the DDN. The capabilities include provision and use of ringing, dial tone, and ON-HOOK and OFF-HOOK state signals.

5. In order to packetize voice, the (secure) analog voice from the STU-IIs must be demodulated on the calling STU-II side. On the called STU-II side, voice packets, after disassembly, must be converted to (secure) analog voice. The need for a modem in the VIU, which is compatible with the STU-II modem to minimize interface complexity, thus becomes obvious.

The selected techniques were used in developing the alternative system-level architectures as described in Section 3. The selected techniques are presented in a tabular form shown in Illustration 2-3.

2.4 EVALUATION CRITERIA AND METHODOLOGY

Evaluation criteria are derived from the Requirements Definition. The methodology we have selected to evaluate the alternative system-level architectures of the VIUs to incorporate the STU-II family of secure voice terminals in the DDN I is based on the assignment of "discriminatory" weighting factors to evaluation criteria as discussed in Reference (1). These are summarized in the following.

2.4.1 Evaluation Criteria

The top-level criteria selected for the evaluation are "Effectiveness" and "Implementation." "Effectiveness" will measure benefits expected in a particular architectural alternative and "Implementation" will measure the penalties associated with obtaining this alternative.

control messages from the calling STU-II and the modem, after demodulation, sends it to the Processor Module in a binary digital form. The modem also takes the digital output of the Processor Module which consists of black or clear voice or STU-II control messages from the called STU-II and modulates them for the calling STU-II.

The major functional requirements of the Modem Module are:

1. Demodulation of the STU-II's analog signal (containing black or clear voice or STU-II control messages)

2. Modulation of the Processor Module's digital output (containing black or clear voice or STU-II control messages)

3. Provide necessary interfaces to support the VDR of 2.4 Kbps. This Modem Module must be equivalent to the modem used in the STU-IIs to minimize any interfacing problems.

3.2.2.2 Interface Requirements of the Modem Module

The Modem Module interfaces must support the following major requirements:

1. Input (from STU-II 2- and 4-wire ports) - black or clear analog signal

2. Output (to the Processor Module) - black or clear digital data

3. Input (from the Processor Module) - black or clear digital data

4. Output (to STU-II 2- and 4-wire ports) - black or clear analog signal.

2. Outputs (to the Processor Module) - OFF-HOOK or ON-HOOK message and Dial Pulse or DTMF message

3. Inputs (from the Processor Module) - busy or ringing message indication

4. Outputs (to the PBX) - busy or ringing signal.

3.2.1.2.3 Interface Requirements of the Generic PBX

The services required of the generic PBX will include, in addition to providing voice path, providing busy or ringing signals, sensing OFF-HOOK or ON-HOOK conditions and passing Dial Pulse or DTMF signals in the format required by the S/S-II Module.

The generic PBX interfaces must support the following major requirements:

1. Inputs (from STU-II) - OFF-HOOK or ON-HOOK signals and Dial Pulse or DTMF signals

2. Outputs (to the S/S-II Module) - OFF-HOOK or ON-HOOK signals and Dial Pulse or DTMF signals

3. Inputs (from the S/S-II Module) - busy or ringing signal

4. Outputs (to STU-II) - busy and ringing signal

5. Inputs (from the Modem Module and STU-II) - black or clear voice and STU-II control messages

6. Outputs (to the Modem Module and STU-II) - black or clear voice and STU-II control messages.

3.2.2 Modem Module

3.2.2.1 Functional Requirements of the Modem Module

The Modem Module is responsible for the demodulation of analog output of the calling STU-II and the modulation of the digital data from the called STU-II. The analog output consists of encrypted (black) or unencrypted (clear) voice or STU-II

1. Provision of a cut-through (pipeline-type) connection through the PBX for a STU-II using inherent capabilities of the generic PBX. This, in effect, will make PBX look like a direct connection as in the VIU with the S/S-I.
2. Use of as much signaling and supervision capability in the generic PBX as possible.

3.2.1.2.1 Functional Requirements of the S/S-II Module

The S/S-II Module will be responsible for converting the signaling and supervision information received from the PBX and relaying this information, after conversion to a suitable binary digital format, to the Processor Module (and vice versa) allowing the services that are normally provided by the PBX to be used in the VIU (see Paragraph 3.2.1.1.1 for services provided).

Specifically the S/S-II Module provides the following major functions:

1. Sends the ON-HOOK or OFF HOOK and Dial Pulse messages to the Processor Module from the PBX
2. Inform the PBX that the called STU-II has returned a busy or ringing signal when the Processor Module sends it a message to do so
3. When using the DTMF signal from the PBX, converts it into a binary digital format for use by the Processor Module.

3.2.1.2.2 Interface Requirements of the S/S-II Module

The S/S-II Module interfaces must support the :ollowing major requirements:

1. Inputs (from the PBX) - OFF HOOK or ON-HOOK signal and Dial Pulse or DTMF signal

3.2.1.1 S/S Type I (S/S-I) Module

3.2.1.1.1 Functional Requirements of the S/S-I Module

The S/S-I Module will be responsible for providing the services that are normally provided by a Central Office. These services include providing busy or ringing signals, sensing ON-HOOK or OFF-HOOK conditions, and passing Dial Pulse or Dual Tone Multifrequency (DTMF) signals in the proper binary digital format required by the Processor Module.

Specifically the S/S-I Module provides the following major functions:

1. Send the ON-HOOK or OFF-HOOK and Dial Pulse messages to the Processor Module
2. Provide the STU-II a busy or ringing signal when the Processor Module sends a message to do so
3. When using the DTMF signal, converts it into a binary digital format for use by the Processor Module.

3.2.1.1.2 Interface Requirements of the S/S-I Module

The S/S-I Module interfaces must support the following major requirements:

1. Inputs (from STU-II) - OFF-HOOK or ON-HOOK signal and Dial Pulse or DTMF signal
2. Outputs (to the Processor Module) - OFF-HOOK or ON-HOOK message and Dial Pulse or DTMF message
3. Inputs (from the Processor Module) - busy or ringing message indication
4. Outputs (to STU-II) - busy or ringing signal.

3.2.1.2 S/S Type II (S/S-II) Module

Interfacing the STU-IIs behind a PBX is driven by the two general principles:

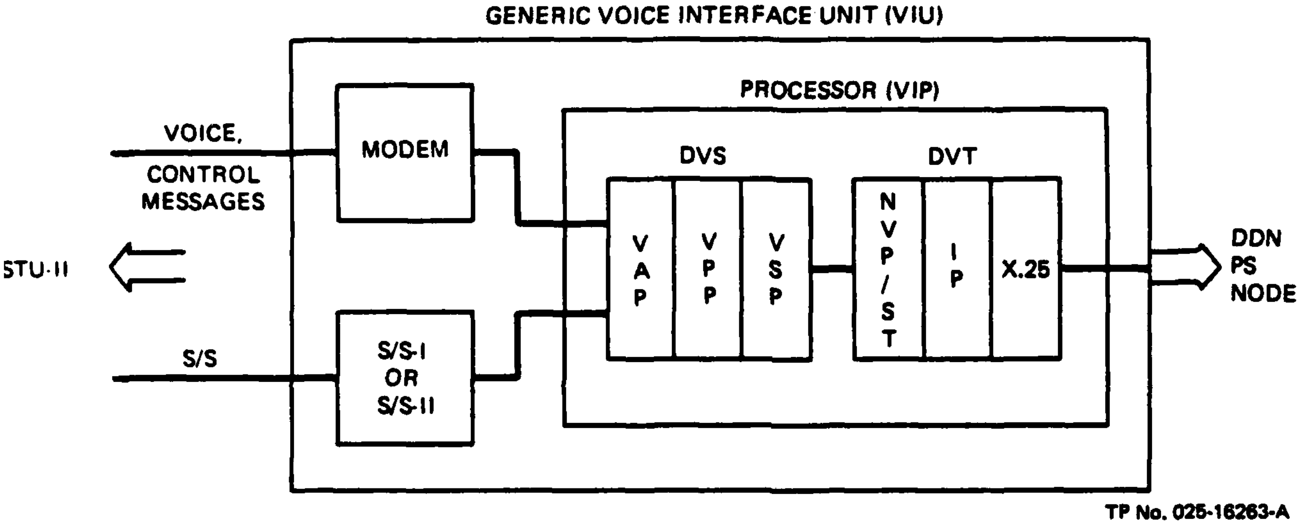


Illustration 3-1. Basic Components of the Generic Voice Interface Unit

In the secure mode of operation the STU-IIs provide black (encrypted) voice. End-to-end security is an inherent capability provided in the STU-IIs which incorporates a concept of call variable for black voice in two modes of their operation, KDC and NET. The STU-IIM provides three outputs: a 4-wire black analog, a 2-wire black analog, and a black digital port. The standard STU-II provides only the 2-wire port. In the 4-wire output configuration the signaling/supervision can be obtained from the E and M lines and the black analog voice and STU-IIM control messages from the R (Receive) and T (Transmit) lines. In the 2-wire configuration the signaling/supervision and voice are on the same lines. The black digital port cannot be used since it provides no signaling/supervision information.

In the non secure mode of operation, STU-IIs can be operated as ordinary telephone units allowing clear (unencrypted) calls to be made.

3.2 BASIC COMPONENTS OF THE GENERIC VOICE INTERFACE UNIT (VIU)

The three major modules of the Generic VIU (Illustration 3-1) are:

1. Signaling and Supervision (S/S) Module
2. Modem Module
3. Processor Module [also called Voice Interface Processor (VIP)].

These modules are described in terms of their functional and interface requirements.

3.2.1 Signaling and Supervision (S/S) Module

The S/S Module can be of Type I or Type II. S/S Type I (S/S-I) is used for direct interfacing of STU-IIs and S/S Type II (S/S-II) Module is used for interfacing when STU-IIs are behind a PBX.

SECTION 3 - SYSTEM-LEVEL ARCHITECTURES TO INCORPORATE STU-IIs IN THE DDN I

Alternative system-level architectures to incorporate the STU-II family of secure voice terminals (called STU-IIs henceforth in the Section unless specific reference to STU-II, STU-IIM, or their enhancement is required) in the DDN I, are defined in this Section. These can be grouped under two major catagories of interfacing options: interfaces using ST agents (and supporting protocols) in the DDN I PS nodes and gateways and interfaces (without ST agents) employing the DDN I as a circuit switched (CS) emulator. All architectures will employ Voice Interface Units (VIU) with STU-IIs being directly connected to them or via a Private Branch Exchange (PBX). All VIUs employ three basic modules (with some variations); Signaling and Supervision (S/S) Module, Modem Module, and a Processor Module made up of either one or two processors. They are responsible for communications between the STU-II and DDN I and provide all necessary functions, interfaces, and protocols to support the communications (see Paragraph 3.2 for details). The alternative system-level architectures are discussed in Paragraph 3.3. Key features of the STU-IIs, which drive the design of the architectures are briefly introduced in Paragraph 3.1 (see classified Appendix D provided in a separate document for details).

3.1 KEY FEATURES OF STU-IIs

The STU-IIs provide voice processing which employs the DoD STD LPC-10 algorithm for voice analysis and synthesis to generate a voice frame of 54 bits contained in a time-interval of 22.5 milliseconds (ms) effectively yielding a voice digitization rate (VDR) of 2.4 Kbps.

Mathematically, this score (S_k) of alternative A_k can be expressed as:

$$S_k = \frac{1}{100} \sum_j w_j \times \sum_i (w_i \times s)_{ijk}$$

Where:

w_i = Weight of lowest level evaluation criiteria in Level i

s_{ijk} = Raw score of alternative A_k in Level i criteria

w_j = Weight of evaluation criteria in Level j

100 = A factor used for normalization.

Alternatives with the highest scores are viable, feasible candidates for further in-depth analysis using future modeling and simulation or test-bed efforts. Alternatives can also be plotted on the graph with "Effectiveness" and "Implementation" on Y- and X- axis respectively. The evaluation details are presented in Section 4.

value of the criteria. An example is an evaluation of personal computers for scientific/word-processing application. Since all of them are generally in the same price range, cost will receive the lowest weight not because it is unimportant in the absolute sense. However, it is not as good a discriminator as the software packages available for scientific/word processing application which will be assigned a high weight.

Weights associated with the evaluation criteria, shown in Illustration 4-1 as percentages, were arrived at using the expert opinion technique in consultation with the Government Task Officer. In the expert opinion technique inputs from a panel of experts at CSC were solicited and final weights arrived at after iterative refinements. These weights add up to a value of 100 at the top level. For example, in the task investigation, since "Implementation" is of far greater importance than "Effectiveness", their weights were respectively 80 and 20, adding to 100 at the top level. Scoring of an alternative will be done as follows.

Scoring of an alternative architecture for the VIUs will be performed starting at the lowest level of criteria by expressing the performance of this architecture in terms of its utility (score on how well) in that criteria. Lowest ranked alternative will get a raw score of "0" and the highest ranked alternative a "100". When such absolute scores cannot be determined, a step scoring will be used; for example a "25" corresponding to "poor", a "50" for "average", a "75" for good, and a "100" for "excellent". These raw scores in various evaluation criteria at the lowest level will be summed up, after multiplying them with the weights of evaluation criteria, to arrive at a score at that level which will be used in the next higher level. This scoring continues to Level 1 criteria wherein, effectively, all weighted lower level scores are collapsed into a single number that gives the score for that alternative.

LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4
1. EFFECTIVENESS	1. WORLDWIDE SURVIVABILITY	1. INVULNERABILITY	NOT APPLICABLE (NA)
		2. SURVIVABILITY MEASURES	1. CALL COMPLETION RATE (VOICE) OR 2. PROBABILITY OF CORRECT MESSAGE DELIVERY (DATA)
		3. RESTORABILITY	NA
	2. SECURITY	1. PASSIVE INTERCEPT RESISTANCE	
		2. SPOOFING RESISTANCE	NA
		3. TRAFFIC ANALYSIS	
		4. KEY PROTECTION	1. STORAGE METHOD 2. LOADING METHOD 3. TRANSMISSION METHOD } NA
		5. UNAUTHORIZED ACCESS	NA
		6. CERTIFICATION	
	3. PERFORMANCE	1. TIMELINESS	1. CALL SETUP TIME (VOICE) OR 2. SPEED OF SERVICE (DATA AND VOICE PACKETS)
		2. QUALITY	1. INTELLIGIBILTY AND NATURALNESS (VOICE) 2. BIT ERROR RATE (DATA)
	4. RESPONSIVENESS	1. INTEROPERABILITY	NA
		2. ADAPTABILITY	
IMPLEMENTATION	1. Δ-COST*	1. PRIMARILY IMPLEMENTATION	
	2. RISK	1. TECHNICAL	
		2. SCHEDULE	

NOTE * INCREMENTAL COST TO THE PLANNED DDN I TO INCORPORATE SECURE VOICE

TP No. 025-16262-A

Illustration 2-4. Evaluation Criteria

These two top-level criteria are further subdivided into as many lower level criteria as required until some "score" or "judgement" can be associated with the selected lower level criteria (see Illustration 2-4). An example is Timeliness criteria (a Level 3 criteria of Effectiveness). It has been subdivided into two Level 4 criteria, call setup time (voice) and speed of service (voice packets) to whom scores can be assigned in different alternative architectures.

Many criteria in the Illustration are marked not applicable (NA) primarily because of the following two reasons.

1. The services/capabilities involved in these criteria are provided external to the alternative system-level architectures of the VIUs

2. The "discriminatory" weights associated with these criteria are zero since all alternative system level architectures of the VIUs provide the same service/capability in these criteria.

An example of item (1) is the Level 3 criteria, Invulnerability, of Worldwide Survivability which is provided by mechanisms employed external to the VIUs. An example of item (2) is the Interoperability (a Level 3 criteria of Responsiveness) in which all VIUs will allow secure digital voice to be incorporated in the DDN I.

2.4.2 Evaluation Methodology

The selected evaluation methodology eliminates the "subjectiveness" associated with the top level evaluation criteria, "Effectiveness" and "Implementation", by their subdivisions into lower level criteria as explained in Appendix A and by associating weights to evaluation criteria that "discriminate" among the alternatives by expressing the relative

End Capabilities Needed	Selected Technique and Comment
17. Speech reconstitution	Protocols in SW of VIUs. They will implement the following major features: a. Sequence numbers and time stamps on voice packets containing voice frames to reassemble speech at called party b. Selected speech reconstitution algorithms, if feasible (to work with the STU-II LPC-10 synthesizer)
18. KDC (voice) and STU-II addressing	Protocols in SW of VIUs
19. DDN access	Protocols in SW of VIUs
20. Cryptosynchronization	Protocols in SW of VIUs for bit-stuffing for lost packet (to maintain bit count integrity) and integral voice frames (out of LPC-10) per voice packet.

Illustration 2-3. Proposed Techniques to Satisfy Required Additional Requirements and End Capabilities (Page 3 of 3)

End Capabilities Needed	Selected Technique and Comment
12. Generation of appropriate signals for dial tone, ringing, etc.	Signaling and Supervision (S/S) Unit HW (see Section 3) in VIUs
13. Near real-time speech delivery	Protocols in SW of the VIUs. This SW will implement the following features to provide the needed end capability: a. Protocols in the SW of the VIUs based on Stream (ST) Protocol and Network Voice Protocol (NVP). The ST allows for a backbone pipeline (a per call permanent virtual circuit) to be setup for a call using ST agents in the PS nodes and gateways of the DDN I (when used). Call initiation and termination, connection setup, and negotiations (if needed), and voice packet transport are also supported by the protocols b. Assignment of highest precedence to voice packets c. Minimization of the size voice packets containing voice frames in a talkspurt by employing minimum protocol overhead (OH) d. Error detection and correction on selected packets carring control messages with absolutely no error correction on voice packets
14. SAD	Not employed
15. Statistical Multiplexing	DDN I PS node
16. Voice packet assembly and disassembly	Protocols in SW of the VIUs

Illustration 2-3. Proposed Techniques to Satisfy Required Additional Requirements and End Capabilities (Page 2 of 3)

End Capability Needed	Selected Technique and Comment
1. Invulnerability	Not Applicable (NA)
2. Survivability	Call completion rate as a measure for voice is required
3. Security	End-to-end security provided in the STU-II family by use of call variables [provided by KDC (voice) or prestored (NET mode)] and/or/both by use of IPLI
4. Performance	Call setup time and speed of service (voice packets) for Timeliness and Intelligibility and Naturalness for Quality as measures for voice are required
5. Interoperability	Use of voice interface units (VIU)
6. Call initiation and termination	HW and protocols in SW of VIUs
7. Connection setup and negotiations	Mostly protocols in SW of VIUs
8. Digital voice packetization	Integral number of voice frames (out of LPC-10) in a voice packet achieved by protocols in SW of VIUs. This will allow for cryptosynchronization to be maintained between the calling and called STU-IIs
9. Voice packet transport	Protocols in SW of VIUs and DDN I backbone facility
10. Buffers	Provided by processor unit(s) (external and/or TAC) (see Section 3) of VIUs
11. Binary digital code translation	Protocols in SW of the VIUs

Illustration 2-3. Proposed Techniques to Satisfy Required Additional Requirements and End Capabilities (Page 1 of 3)

3.2.3 Processor Module

3.2.3.1 Functional Requirements of the Processor Module

The Processor Module includes buffers, binary digital code translator, Data Voice Server (DVS) function, and Data Voice Transfer (DVT) function to support STU-IIs interfacing to the DDN PS node and allow for end-to-end transfer of secure voice between calling and called STU-IIs.

Thc buffers support voice frames assembly into voice packets (by method of counting bits when black voice is used), non-blocking voice frames storage (within a call), and storage to support speech reconstitution in the STU-IIs.

The translator supports conversion of DDN binary codes to digits which can be used by the S/S and/or Modem Modules for appropriate actions by STU-IIs and vice versa.

The DVS function will process all of the S/S, black or clear digital voice, and STU-II control messages using the resident high level protocols (VAP, VPP, and VSP) and translate them into an information that can be used by network transport and access protocols (NVP/ST, IP, and X.25) in the DVT function (see Appendix C for details).

The NVP [Reference (12)] and ST [Reference (13)] are the recommended protocol counterparts to the presently defined DDN data protocols TCP and IP [Reference (8) and (7) respectively] at the transport and internet levels, to support near real-time speech delivery (see Illustration C-16). The special NVP/ST protocol has been developed during the task investigation based on the ST protocol. It controls the transmission of a digital representation of voice signals through a packet-switched network in near real-time. This is achieved by establishing a permanent virtual circuit (PVC) through the network during a connection setup, allowing the established PVC connection for negotiations (a capability not required in this investigation), and transmitting all voice packets in that call over this PVC connect'on when calling and called parties agree in negotiations. The technique used in this process (ST agents in the DDN PS nodes and gateways) allows the header of a packet to be much smaller, thus reducing the overhead processing time and delay (see Paragraph C.2.4 of Appendix C for details on the NVP/ST).

The major Processor Module functional requirements are:

1. Support call initiation as follows:

   a. The DVS receives the number to be called from the S/S Module

   b. The DVS looks up the corresponding DDN directory number from a stored table and sends it to the NVP/ST protocol in the DVT for connection setup.

2. Establish a per-call logical connection using the Voice Session Protocol (VSP) in the DVS and physical connection (a PVC) using the NVP/ST protocol in the DVT (with ST agents support when they are used)

3. Support calling and called party negotiations using the Voice Presentation Protocol (VPP) in the DVS

4. Provide for the packetization of black or clear voice frames and STU-II control messages for transmission over the PVC connection, which is performed by the Voice Application Protocol (VAP) in the DVS on the calling STU-II side

5. Detection of lost packets and their replacement with packets containing the same number of bits sent to maintain bit count integrity (all packets will contain the same number of bits for this reason), which will be

the responsibility of the VAP in the DVS on the called STU-II side (using time-stamp and sequence numbers) to maintain cryptosychronization

6. Ensure adequate delay for speech reconstitution (in the STU-IIs) by the use of buffers, time-stamp, and sequence number information under the control of the DVS

7. Provide interfaces to DDN I supporting the exchange of X.25 frames between the Processor Module and the DDN I PS node. The frame format at the data link level is shown in Illustration 3-2.

F	A	C	X.25 Level Header	IP Header	NVP/ST Header	Data	FCS	F

Where: F - 8-bit flag
A - 8-bit address
C - 8-bit control
FCS - Frame Check Sequence (16 bits)

Illustration 3-2. Frame Format at Data Link Level

8. Monitor and control the activities of all modules in the VIU

9. Generate appropriate control signals for proper communications between all modules of the VIU

10. Maintain proper timing among all modules of the VIU.

3.2.3.2 Interface Requirements of the Processor Module

The Processor Module interfaces must support the following major requirements:

1. Inputs:

   a. Dial Pulse or DTMF message (from the S/S Module)

   b. OFF-HOOK or ON-HOOK message (from the S/S Module)

c. Ringing or busy message (from the called STU-II)

d. Black or clear digital voice (from the Modem Module)

e. STU-II control messages (from the Modem Module)

f. Messages required for the DVS to the DVT communication and vice versa using the proposed protocols (see Appendix C)

g. Status from all modules within the VIU

h. The S/S or Modem Module activity indication for the Processor Module activation.

2. Outputs:

a. (NVP/ST)/IP/X.25 formatted messages (to the PS node) (Illustration 3-2)

b. Ringing or busy message indication (to the S/S Module)

c. Black or clear digital voice (to the Modem Module)

d. STU-II control messages (to the Modem Module)

e. Messages required for the DVT to the DDN PS node communication and vice versa using the proposed protocols

f. Appropriate control signals to all modules within the VIU.

3.3 ALTERNATIVE SYSTEM-LEVEL ARCHITECTURES

In this paragraph, the alternative system-level architectures to incorporate secure voice as provided by the STU-IIs in the DDN I, are described. All architectures employ the S/S-I or II Module, Modem Module, and Processor Module [also called the Voice Interface Processor (VIP) Module] which are detailed in Paragraph 3-2.

The system-level architectures can be grouped under two major categories of interfacing options: interfaces using ST agents in the DDN I PS nodes and gateways and interfaces without using ST agents. In the former, the DDN I backbone is employed as a PS network, and in the latter option, as a CS emulator. Additional major subcategories (a total of 48) result from the combinations of the following features (see Illustration 3-3).

1. End-to-end security architecture employed (NET mode of STU-IIs and/or IPLIs)
2. The type of processor used in the Processor Module (or VIP) of the VIU [DDN I supplied TAC and/or external processor(s)]
3. Direct connection of STU-IIs versus connection of the STU-IIs when they are behind a PBX. The S/S-I is required for Direct connection and S/S-II, for Behind the PBX connection.

The major advantages and disadvantages in using these features are as follows:

ST Agents Versus No ST Agents

ST agents will provide a near real-time speech delivery in the DDN I at the expense of higher cost for their implementation in the DDN I PS nodes and gateways. Without the ST agents there is no guarantee on near real-time speech delivery; however, the cost for implementation in this option is smaller compared to that with the ST agents.

End-to-end Security Architecture Employed

In the NET mode of STU-IIs, the inherent capability in the STU-IIs to provide an end-to-end security is employed. The problem encountered in this end-to-end security architecture is the need to implement a mechanism on the called STU-II side to maintain cryptosynchronization. End-to-end security

SUBCATEGORY NUMBER	ST AGENTS		END TO END SECURITY ARCHITECTURE			PROCESSOR USED IN THE PROCESSOR MODULE				STU-II CONFIGURATION FOR INTERFACING	
	YES	NO	IPLI	NET	IPLI + NET	TAC	ONE P	TAC + ONE P	TWO P	DIRECT	BEHIND-THE-PBX
1 THROUGH 48 CORRESPONDING TO 48 COMBINATIONS	2 COMBINATIONS		3 COMBINATIONS			4 COMBINATIONS				2 COMBINATIONS	

TP No. 026-16538-A

NOTE: P STANDS FOR EXTERNAL PROCESSOR

Illustration 3-3. Major Subcategories of the System-Level Architectures architecture, employing the IPLIs avoids this problem by using IPLIs to encrypt/decrypt clear voice from/to STU-IIs; however, there is a cost penalty associated with the IPLIs acquistion to support secure end-to-end voice transmission. Certification is also an issue when IPLIs are used for voice packets since, at present, they are certified for use with data packets only. In the end-to-end security architecture employing the NET mode of STU-IIs and IPLIs, security is maximum because of the double encryption employed with the problems for both the NET mode and use of IPLIs alone attendant.

Type of Processor Used in the VIP

The type of processor used in the Processor Module (or the VIP) of the VIU presents the following situation.

1. The TAC used as the VIP - the major advantages of using the TAC are:

   a. There is no additional cost involved to acquire it

   b. The TAC already contains the X.25 and IP protocols (which are needed in the proposed protocol architecture) and it has been used in the ARPANET for many years

   c. The TAC also contains the TCP for future packet voice and data integration when SAD is possible and economically feasible with the secure voice terminals used.

The major drawback in using the TAC is getting the software for the proposed protocol architecture implemented in it.

2. External Processor Used as the VIP - The major advantages of using the external processor are:

   a. There is no dependence on having the TAC available at sites where VIUs are to be implemented

   b. A high degree ɔf flexibility is possible in designing and implementing the proposed protocol architecture

   c. External processor hardware can be selected to match very closely the requirements for implementing the desired secure voice capability in the DDN I.

The major drawback in using the external processor is the cost of acquiring it.

3. The TAC and an External Processor Used as the VIP - The major advantage of using the TAC and one external processor is that the TAC supports the X.25 and IP protocols. Only the NVP/ST protocol (in the TAC) and higher level protocols; VAP, VPP, and VSP; need be developed in the external processor.

The major drawback in using the TAC and one external processor is the additional interfaces that will result from the TAC to external processor communications.

4. Two external processors used as the VIP - The major advantage of using two external processors is the total flexibility obtained in designing and implementing the proposed protocol architecture. For example, the DVS can be implemented in one external processor and the DVT in the other.

The major drawbacks in using two external processors are:

   a. Highest cost penalty to acquire the two processors

The major drawback in using the TAC is getting the software for the proposed protocol architecture implemented in it.

2. External Processor Used as the VIP - The major advantages of using the external processor are:

   a. There is no dependence on having the TAC available at sites where VIUs are to be implemented

   b. A high degree of flexibility is possible in designing and implementing the proposed protocol architecture

   c. External processor hardware can be selected to match very closely the requirements for implementing the desired secure voice capability in the DDN I.

The major drawback in using the external processor is the cost of acquiring it.

3. The TAC and an External Processor Used as the VIP - The major advantage of using the TAC and one external processor is that the TAC supports the X.25 and IP protocols. Only the NVP/ST protocol (in the TAC) and higher level protocols; VAP, VPP, and VSP; need be developed in the external processor.

The major drawback in using the TAC and one external processor is the additional interfaces that will result from the TAC to external processor communications.

4. Two external processors used as the VIP - The major advantage of using two external processors is the total flexibility obtained in designing and implementing the proposed protocol architecture. For example, the DVS can be implemented in one external processor and the DVT in the other.

The major drawbacks in using two external processors are:

   a. Highest cost penalty to acquire the two processors

2. Possible need to implement X.25 and IP protocol packages

3. Highest degree of interfacing required.

Direct Connection Versus Behind-the-PBX Connection of the STU-IIs to the DDN I

The major advantage of the Behind-the-PBX configuration of the STU-IIs is the increased adaptability it provides in terms of ease of expansion. This is achieved by providing a capability to attach more STU-IIs to the DDN I via the PBX without changing the DDN I connectivity.

Illustration 3-4 summarizes all possible system-level architectures for incorporating the STU-IIs in the DDN I in late 1980s time-frame. With the dashed area/lines convention used in the Illustration, there is no need to provide a separate illustration for each system-level architecture.

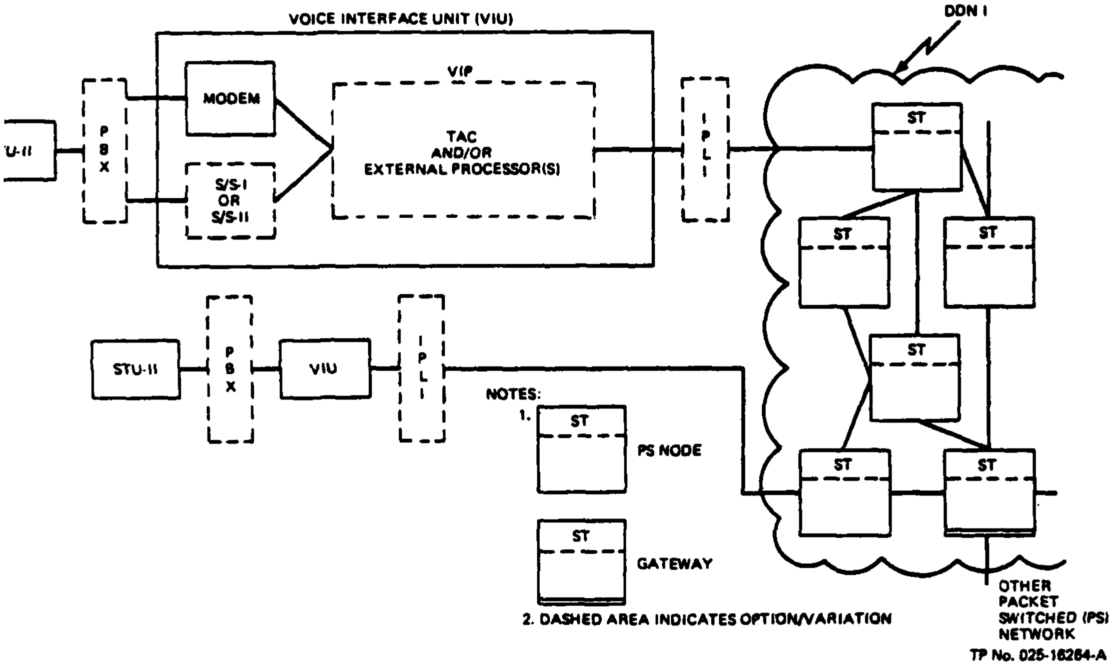


Illustration 3-4. Possible System-level Architectures

SECTION 4 - EVALUATION, RECOMMENDATIONS, AND IMPLEMENTATION

4.1 INTRODUCTION

Evaluation of the alternative system-level architectures described in Section 3, is based on the evaluation criteria and methodology defined in Paragraph 2.4. Recommendations identify the architectures which are candidates for further indepth analyses using modeling and simulation or test-bed implementation. Implementation defines how the recommended architecture, for the selected weight distribution of the evaluation criteria, can be implemented, whether in hardware and software, and their transition and scheduling to incorporate the secure voice capability (as provided by the STU-IIs) in the DDN I in late 1980s time-frame. The following paragraphs describe the details on evaluation, recommendations, and implementation.

4.2 EVALUATION

4.2.1 Scoring For System-Level Architectures

Illustration 4-1 summarizes the weights of the criteria which are used in the evaluation. The weights for Effectiveness and Implementation are respectively identified as y and x to allow for parametric evaluations (or sensitivity analysis) of the architectures, with 20 and 80 as their selected values for the task effort application. The rationale in assigning these weights to Effectiveness and Implementation is that the latter is critical in the DDN I for providing a backup mode of operation for secure voice (employing the VIUs) and in such a mode of operation components of Effectiveness are less important because the architectures are not expected to provide excellent scores in them. Weights associated with the Survivability, Security, Performance, and Responsiveness components of Effectiveness reflect this rationale. Of the two major components of

- Effectiveness (y)[1]
    - Survivability (30)
        - Call Completion Rate (30)
    - Security (40)
        - Passive Intercept Resistance (10)
        - Traffic Analysis (10)
        - Certification (20)
    - Performance (15)
        - Timeliness (7.5)
            - Call Setup Time (3.75)
            - Speed of Service (Voice Packets) (3.75)
        - Quality (7.5)
    - Responsiveness (15)
        - Adaptability (15)
- Implementation (x)[1]
    - Δ -Cost[2] (70)
    - Risk (30)
        - Technical (15)
        - Schedule (15)

Notes:

1. x + y = 100%
2. Incremental cost over the planned DDN I to incorporate VIUs

Illustration 4-1. Weights of Evaluation Criteria Used mplementation, Δ - Cost is assigned a weight of 70 since it was elt that cost is a primary driver while the other component, isk, although important, was a secondary driver with a weight of 0. A further breakdown of the weights, shown in the llustration, is based on our expert opinion technique and onsultation with the Government Task Officer.

Employing these weights, the score (S_k) for an alternative ystem-level architecture (A_k) can be expressed as:

$$S_k = \frac{1}{100} \left\{ (y \sum_i w_{yi} \times s_{ik}) + (x \sum_j w_{xj} \times s_{jk}) \right\}$$

where:

w_{yi} = Weights associated with Effectiveness Components

w_{xj} = Weights associated with Implementation Components

s_{ik} = Raw score of alternative A_k in component yi

s_{jk} = Raw score of alternative A_k in component xj

100 = A factor used for normalization.

This equation was used in the evaluations as follows.

Raw scores (w_{yi}, w_{xj}) were assigned to the architectures as the averages (13, 38, 63, and 88), respectively of the step scoring (P = Poor, A = Average, G = Good, and E = Excellent) used. For example, 13 was arrived at as an average of P given by [(0 + 25)/2] rounded up. This was necessary since without modeling and simulation or testbed, in most cases, qualitative score could not be determined. Small perturbations around the averages were made to indicate the impact of an attribute on an architecture in a particular evaluation criteria. An example of this is an increase in score of 2 in Δ -Cost score for architectures without ST agents over the Δ - cost score for architectures with ST agents because of less cost in the former as a result of no need for the ST implementation (the attribute in this case).

	TYPE 1 BEHIND PBX			TYPE 2 BEHIND PBX			TYPE 3 BEHIND PBX			TYPE 4 BEHIND PBX		
CUMULATIVE PERFORMANCE WEIGHT	IPLI	NET	IPLI + NET	IPLI	NET	IPLI + NET	IPLI	NET	IPLI + NET	IPLI	NET	IPLI + NET
0	60.5	76.0*	63.5	49.1	64.6	52.1	44.4	59.9	47.4	32.9	48.5	35.9
→ 3.0	60.6	75.6*	63.6	49.6	64.6	52.6	45.0	60.0	48.0	34.0	49.0	37.0
6.0	60.7	75.2*	63.7	50.1	64.6	53.1	45.7	60.2	48.7	35.1	49.6	38.1
12.0	60.9	74.3*	63.9	51.2	64.6	54.2	47.1	60.5	50.1	37.3	50.8	40.3
20.0	61.2	73.2*	64.2	52.5	64.6	55.5	48.9	61.0	51.9	40.3	52.3	43.3
30.0	61.6	71.0*	64.6	54.3	64.5	57.3	51.2	61.5	54.2	44.0	54.2	47.0
50.0	62.3	69.0*	65.3	57.7	64.5	60.7	55.0	62.6	58.8	51.3	58.1	54.3

	TYPE 5 BEHIND PBX			TYPE 6 BEHIND PBX			TYPE 7 BEHIND PBX			TYPE 8 BEHIND PBX		
CUMULATIVE PERFORMANCE WEIGHT	IPLI	NET	IPLI + NET	IPLI	NET	IPLI + NET	IPLI	NET	IPLI + NET	IPLI	NET	IPLI + NET
0	60.3	75.8	63.3	48.9	64.4	51.9	44.1	59.7	47.1	32.7	48.2	35.7
→ 3.0	59.6	74.6	62.6	48.6	63.6	51.6	44.0	59.0	47.0	33.0	48.0	36.0
6.0	58.9	73.4	61.9	48.3	62.8	51.3	43.9	58.4	46.9	33.3	47.8	36.3
12.0	57.5	71.0	60.5	47.8	61.2	50.8	43.7	57.2	46.7	34.0	47.4	37.0
20.0	55.7	67.7	58.7	47.1	59.1	50.1	43.5	55.5	46.5	34.8	46.8	37.8
30.0	53.4	63.7	56.4	46.2	56.4	49.2	43.1	53.4	46.1	35.8	46.1	38.8
50.0	48.9	55.7	51.9	44.4	51.1	47.4	42.5	49.3	45.5	37.9	44.7	40.9

NOTES: 1. * Indicates optimum scores
2. → Indicates selected cumulative weight

Illustration 4-10. Sensitivity of Scores With Respect to Performance Criteria Weight Variation

CUMULATIVE DELTA-COST WEIGHT	TYPE 1			TYPE 2			TYPE 3			TYPE 4		
		BEHIND PBX			BEHIND PBX			BEHIND PBX			BEHIND PBX	
	IPLI	NET	IPLI + NET	IPLI	NET	IPLI + NET	IPLI	NET	IPLI + NET	IPLI	NET	IPLI + NET
0	53.9	57.7	65.3	56.9	60.7	68.3*	52.3	56.1	63.7	55.3	59.1	66.7
20.0	56.3	64.1	64.7*	54.3	62.1	62.7	49.7	57.5	58.1	47.7	55.5	56.1
30.0	57.5	67.3*	64.4	53.0	62.8	59.9	48.4	58.2	55.3	43.9	53.7	50.8
→ 56.0	60.6	75.6*	63.6	49.6	64.6	52.6	45.0	60.0	48.0	34.0	49.0	37.0
70.0	62.3	80.1*	63.2	47.8	65.6	48.7	43.2	61.0	44.1	28.7	46.5	29.6
75.0	62.9	81.7*	63.0	47.1	65.9	47.3	42.6	61.4	42.7	26.8	45.6	27.0

CUMULATIVE DELTA-COST WEIGHT	TYPE 5			TYPE 6			TYPE 7			TYPE 8		
		BEHIND PBX			BEHIND PBX			BEHIND PBX			BEHIND PBX	
	IPLI	NET	IPLI + NET	IPLI	NET	IPLI + NET	IPLI	NET	IPLI + NET	IPLI	NET	IPLI + NET
0	44.4	48.2	55.8	47.4	51.2	58.8	42.9	46.7	54.3	45.9	49.7	57.3
20.0	49.8	57.6	58.2	47.8	55.6	56.2	43.3	51.1	51.7	41.3	49.1	49.7
30.0	52.6	62.4	59.5	48.1	57.9	55.0	43.5	53.3	50.4	39.0	48.8	45.9
→ 56.0	59.6	74.6	62.6	48.6	63.6	51.6	44.0	59.0	47.0	33.0	48.0	36.0
70.0	63.4	81.2	64.3	48.9	66.7	49.8	44.3	62.1	45.2	29.8	47.6	30.7
75.0	64.7	83.5	64.9	49.0	67.8	49.1	44.4	63.2	44.6	28.7	47.5	28.8

<u>NOTES:</u> 1. * Indicates optimum scores
2. → Indicates selected cumulative weight

Illustration 4-9. Sensitivity of Scores With Respect to Δ -Cost Criteria Weight Variation

Illustration 4-9 and 4-10 wherein sensitivity analysis is conducted, respectively, with respect to Δ - Cost and Performance criteria weight variations. Astericks (*) identify the optimum architectures (with highest scores) in the Illustrations.

4.3 RECOMMENDATIONS AND IMPLEMENTATION

4.3.1 Recommendations

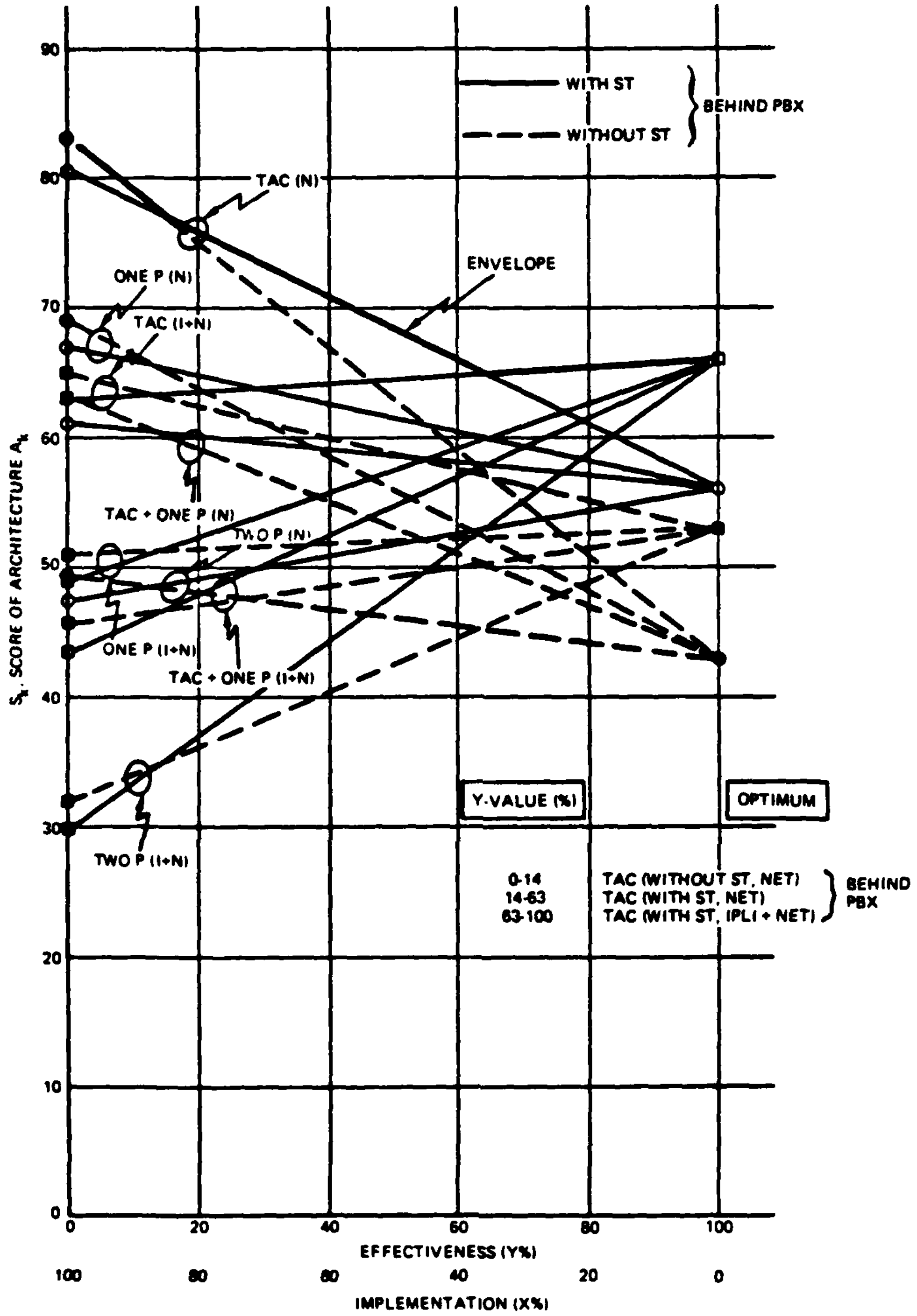
Sensitivity analysis of the scores of architectures with respect to Effectiveness criteria weight indicates that, for practical effectiveness criteria weight range (14-63%), Type 1 architecture (with ST, Behind-the-PBX, NET) is the optimum alternative (the final recommendation). At the low end of effectiveness, the Type 5 architecture which differs from the recommended Type 1 architecture in that it does not employ ST agents, is the optimum alternative (see Illustration 4-8). At the high end of effectiveness, the Type 1 architecture which differs from the recommended Type 1 architecture in that an additional security (double encryption) is provided using IPLI + NET mode of security architecture, is the optimum alternative.

We have also observed in Illustration 4-5 that the scores for architectures with Behind-the-PBX interfacing are slightly better than the scores of the corresponding architectures with Direct interfacing. Therefore, we conclude that, for weight distributions of the evaluation criteria, all Type 1 architectures for higher end of effectiveness and Type 5 architectures for lower end of effectiveness be explored further for the optimum alternatives.

However, for the selected weight distribution of the evaluation criteria, the recommendation for implementation is the Type 1 architecture with ST agents in the DDN I PS nodes and gateways using Behind-the-PBX interfacing and NET mode of security architecture (see Illustration 4-5). This architecture employs the TAC as a Processor Module in the VIU.

Effectiveness Weight Range	Architecture With Optimum Score
0-14%	Type 5 (Without ST, Behind PBX, NET)
14-63%	Type 1 (With ST, Behind PBX, NET)
63-100%	Type 1 (With ST, Behind PBX, IPLI + NET)

Illustration 4-8. Architectures With Optimum Scores



TP No. 025-18272-A

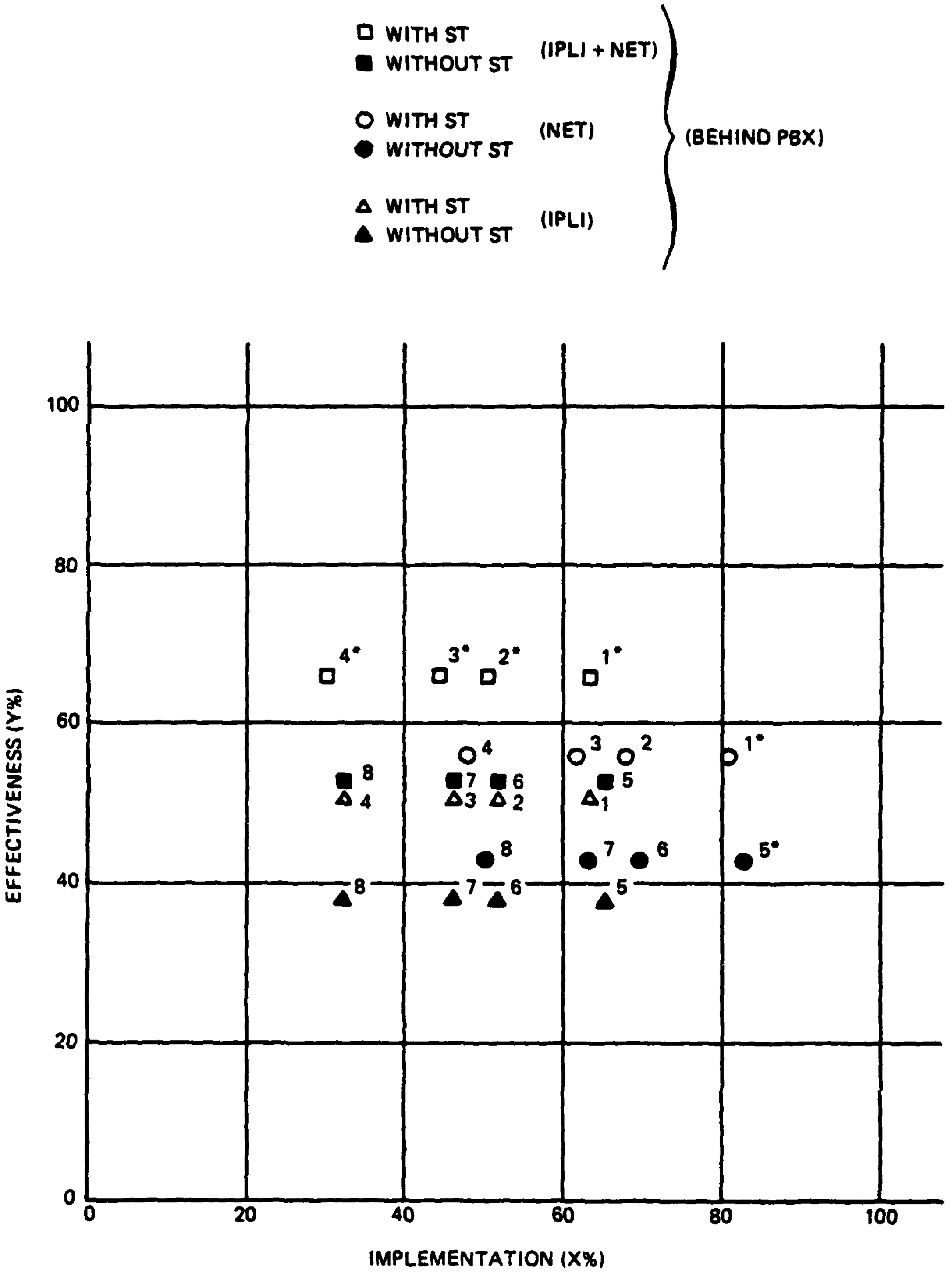
Illustration 4-7. Sensitivity Analysis of Scores of Architectures with Variation in Effectiveness and Implementation Criteria Weights

The third step in the analysis was to conduct sensitivity analysis or to plot the parametric variation of the score, S_k, of an architecture, A_k, with respect to effectiveness and implementation criteria weights variation, for the subset of 16 architectures (Types 1 through Type 8 employing security architectures, involving either NET mode or IPLI + NET mode (Illustration 4-7). These include the set of six architectures identified in the second step. A more comprehensive set was chosen to ensure that in arriving at the architectures with optimum (highest) scores using the parametric variation, a candidate architecture for recommendation is not left out. The outer envelope of the plot in the Illustration indicates the set of architectures with optimum scores, for selected criteria weights, as summarized in Illustration 4-8.

At the low end of Effectiveness (0-14% range), Type 5 (without ST, Behind PBX, NET) architecture has the optimum score primarily because Implementation is the major concern (as reflected by Without ST implementation.) In the Effectiveness range of (14-63%), Type 1 (With ST, Behind PBX, NET) architecture has the optimum score with a good balance obtained between Performance and Δ-Cost using, respectively ST agents and NET mode of security architecture. At the high end of Effectiveness (63-100% range), Type 1 (With ST, Behind PBX, IPLI + NET) architecture has the optimum score because of additional security (double encryption) provided by IPLI + NET mode of security architecture above that provided by the architecture in the previous range.

4.2.3 Additional Detailed Analysis

Additional sensitivity analysis of the scores of the architectures can also be conducted with a variation in the lower level criteria weights. Two examples of this are shown in



TP No. 025-16268-A

Illustration 4-6. Effectiveness Versus Implementation

	Interfacing ➡	Direct			Behind PBX		
Type ⬇	Security ➡	IPLI + NET	NET	IPLI	IPLI + NET	NET	IPLI
1	With ST	62.8	74.8	59.8	63.6	75.6*	60.6
2		51.8	63.8	48.8	52.6	64.6	49.6
3		47.2	59.2	44.2	48.1	60.1	45.1
4		36.2	48.2	33.2	37.1	49.1	34.1
5	Without ST	61.7	73.7	58.7	62.6	74.6	59.6
6		50.8	62.7	47.7	51.6	63.6	48.6
7		46.2	58.2	43.2	47.0	59.0	44.0
8		35.2	47.2	32.2	36.0	48.0	33.0

* Optimum (highest) score

Illustration 4-5. Scores for Architectures With Selected Criteria Weight Distribution

4.2.2 Steps Used in the Analysis of the Scoring for System-Level Architectures

As a first step in the analysis, the scores of the architectures obtained by employing the selected weights of the criteria were examined (see Illustration 4-5). The following major conclusions can be drawn from the scores in the Illustration:

1. Architectures with ST agents perform better than the corresponding architectures without ST agents
2. Within a given Type of architecture (Type 5 as an example), architectures with Behind-the-PBX interfacing perform better than the corresponding architectures with Direct interfacing
3. Within a given Type of architecture (Type 1 as an example), architectures with NET mode of security architecture and Behind the PBX interfacing perform the best.

A further evaluation is needed to arrive at the optimum set of architectures for the selected weight distribution of the criteria.

As a second step in the analysis, effectiveness scores are plotted on y-axis with implementation scores on the x-axis as shown in Illustration 4-6. Note that only those architectural subcategories employing the Behind the PBX interfacing (a total of 24 out of the possible 48) were plotted because they yield better scores than the corresponding architectural subcategories employing the Direct interfacing. The Illustration clearly indicates, for the selected assignment of criteria weights in the Effectiveness and Implementation criteria, that the six architectures lying on the outer envelope of the plot (identified by *) are candidates for further investigation using parametric variation of Effectiveness and Implementation criteria weights.

cost of implementing the protocol architecture in the VIU processor(s) (TAC, or one external processor, or TAC and one external processor, or two external processors), based on the lines of code estimates; the software cost for implementing the ST agents in the DDN I PS nodes and gateways; and the cost of acquiring IPLIs. TAC, if used, was considered available with no cost penalty. As a result, for architectures employing the security architecture involving the NET mode of STU-II operation, the score is highest in Δ -Cost criteria in a given Type of architecture because of the cost penalty associated with the IPLI acquisition in the two other security architectures.

5. Technical Risk was lowest with the Types 1, 2, 5, and 6 architectures employing a single processor (TAC or external processor) in the VIUs; with the TAC, additional protocol software can be easily added, whereas with one external processor a high degree of flexibility in designing and implementing the protocol architecture is possible.

6. Schedule Risk was highest with the Type 1 and 5 architectures (because of enhancements in the existing software of the TAC) and lowest with the Type 4 and 8 architectures (because of the highest degree of flexibility in designing and implementing software in two external processors). This was reflected in the lowest scores associated with Type 1 (and Type 5) architectures and highest scores, with Type 4 (and Type 8) architectures in Schedule Risk criteria.

WITHOUT ST AGENTS

	TYPE 5						TYPE 6					
	DIRECT			BEHIND PBX			DIRECT			BEHIND PBX		
	IPLI	NET	IPLI + NET	IPLI	NET	IPLI + NET	IPLI	NET	IPLI + NET	IPLI	NET	IPLI + NET
EFFECTIVNESS												
SURVIVABILITY												
CALL COMPLETION RATE	13.0	13.0	30.0	13.0	13.0	13.0	13.0	13.0	13.0	13.0	13.0	13.0
SECURITY												
PASSIVE INTERCEPT	63.0	63.0	88.0	63.0	63.0	88.0	63.0	63.0	88.0	63.0	63.0	88.0
TRAFFIC ANAYLIS	63.0	63.0	88.0	63.0	63.0	88.0	63.0	63.0	88.0	63.0	63.0	88.0
CERTIFICATION	30.0	63.0	88.0	30.0	63.0	88.0	30.0	63.0	88.0	30.0	63.0	88.0
PERFORMANCE												
TIMELINESS												
CALL SETUP TIME	66.0	66.0	66.0	73.0	73.0	73.0	66.0	66.0	66.0	73.0	73.0	73.0
SPEED OF SERVICE (VP)	13.0	13.0	13.0	20.0	20.0	20.0	13.0	13.0	13.0	20.0	20.0	20.0
QUALITY	30.0	30.0	30.0	30.0	30.0	30.0	30.0	30.0	30.0	30.0	30.0	30.0
RESPONSIVNESS												
ADAPTABILITY	25.0	25.0	25.0	50.0	50.0	50.0	25.0	25.0	25.0	50.0	50.0	50.0
IMPLEMENTATION												
DELTA-COST	65.0	90.0	65.0	65.0	90.0	65.0	40.0	65.0	40.0	40.0	65.0	40.0
RISK												
TECHNICAL	90.0	90.0	90.0	90.0	90.0	90.0	90.0	90.0	90.0	90.0	90.0	90.0
SCHEDULE	40.0	40.0	40.0	40.0	40.0	40.0	65.0	65.0	65.0	65.0	65.0	65.0

	TYPE 7						TYPE 8					
	DIRECT			BEHIND PBX			DIRECT			BEHIND PBX		
	IPLI	NET	IPLI + NET	IPLI	NET	IPLI + NET	IPLI	NET	IPLI + NET	IPLI	NET	IPLI + NET
EFFECTIVNESS												
SURVIVABILITY												
CALL COMPLETION RATE	13.0	13.0	13.0	13.0	13.0	13.0	13.0	13.0	13.0	13.0	13.0	13.0
SECURITY												
PASSIVE INTERCEPT	63.0	63.0	88.0	63.0	63.0	88.0	63.0	63.0	88.0	63.0	63.0	88.0
TRAFFIC ANAYLIS	63.0	63.0	88.0	63.0	63.0	88.0	63.0	63.0	88.0	63.0	63.0	88.0
CERTIFICATION	30.0	63.0	88.0	30.0	63.0	88.0	30.0	63.0	88.0	30.0	63.0	88.0
PERFORMANCE												
TIMELINESS												
CALL SETUP TIME	66.0	66.0	66.0	73.0	73.0	73.0	66.0	66.0	66.0	73.0	73.0	73.0
SPEED OF SERVICE (VP)	13.0	13.0	13.0	20.0	20.0	20.0	13.0	13.0	13.0	20.0	20.0	20.0
QUALITY	30.0	30.0	30.0	30.0	30.0	30.0	30.0	30.0	30.0	30.0	30.0	30.0
RESPONSIVNESS												
ADAPTABILITY	25.0	25.0	25.0	50.0	50.0	50.0	25.0	25.0	25.0	50.0	50.0	50.0
IMPLEMENTATION												
DELTA-COST	40.0	65.0	40.0	40.0	65.0	40.0	15.0	40.0	15.0	15.0	40.0	15.0
RISK												
TECHNICAL	65.0	65.0	65.0	65.0	65.0	65.0	65.0	65.0	65.0	65.0	65.0	65.0
SCHEDULE	52.0	52.0	52.0	52.0	52.0	52.0	77.0	77.0	77.0	77.0	77.0	77.0

Illustration 4-4. Raw Scores for System-Level Architectures Without ST Agents

WITH ST AGENTS

	TYPE 1						TYPE 2					
	DIRECT			BEHIND PBX			DIRECT			BEHIND PBX		
	IPLI	NET	IPLI + NET	IPLI	NET	IPLI + NET	IPLI	NET	IPLI + NET	IPLI	NET	IPLI + NET
EFFECTIVENESS												
SURVIVABILITY												
CALL COMPLETION RATE	30.0	30.0	30.0	30.0	30.0	30.0	30.0	30.0	30.0	30.0	30.0	30.0
SECURITY												
PASSIVE INTERCEPT	63.0	63.0	80.0	63.0	63.0	80.0	63.0	63.0	80.0	63.0	63.0	80.0
TRAFFIC ANAYLIS	63.0	63.0	80.0	63.0	63.0	80.0	63.0	63.0	80.0	63.0	63.0	80.0
CERTIFICATION	30.0	63.0	80.0	30.0	63.0	80.0	30.0	63.0	80.0	30.0	63.0	80.0
PERFORMANCE												
TIMELINESS												
CALL SETUP TIME	63.0	63.0	63.0	70.0	70.0	70.0	63.0	63.0	63.0	70.0	70.0	70.0
SPEED OF SERVICE (VP)	63.0	63.0	63.0	70.0	70.0	70.0	63.0	63.0	63.0	70.0	70.0	70.0
QUALITY	63.0	63.0	63.0	63.0	63.0	63.0	63.0	63.0	63.0	63.0	63.0	63.0
RESPONSIVNESS												
ADAPTABILITY	30.0	30.0	30.0	63.0	63.0	63.0	30.0	30.0	30.0	63.0	63.0	63.0
IMPLEMENTATION												
DELTA-COST	63.0	80.0	63.0	63.0	80.0	63.0	30.0	63.0	30.0	30.0	63.0	30.0
RISK												
TECHNICAL	80.0	80.0	80.0	80.0	80.0	80.0	80.0	80.0	80.0	80.0	80.0	80.0
SCHEDULE	30.0	30.0	30.0	30.0	30.0	30.0	63.0	63.0	63.0	63.0	63.0	63.0

	TYPE 3						TYPE 4					
	DIRECT			BEHIND PBX			DIRECT			BEHIND PBX		
	IPLI	NET	IPLI + NET	IPLI	NET	IPLI + NET	IPLI	NET	IPLI + NET	IPLI	NET	IPLI + NET
EFFECTIVENESS												
SURVIVABILITY												
CALL COMPLETION RATE	30.0	30.0	30.0	30.0	30.0	30.0	30.0	30.0	30.0	30.0	30.0	30.0
SECURITY												
PASSIVE INTERCEPT	63.0	63.0	80.0	63.0	63.0	80.0	63.0	63.0	80.0	63.0	63.0	80.0
TRAFFIC ANAYLIS	63.0	63.0	80.0	63.0	63.0	80.0	63.0	63.0	80.0	63.0	63.0	80.0
CERTIFICATION	30.0	63.0	80.0	30.0	63.0	80.0	30.0	63.0	80.0	30.0	63.0	80.0
PERFORMANCE												
TIMELINESS												
CALL SETUP TIME	63.0	63.0	63.0	70.0	70.0	70.0	63.0	63.0	63.0	70.0	70.0	70.0
SPEED OF SERVICE (VP)	63.0	63.0	63.0	70.0	70.0	70.0	63.0	63.0	63.0	70.0	70.0	70.0
QUALITY	63.0	63.0	63.0	63.0	63.0	63.0	63.0	63.0	63.0	63.0	63.0	63.0
RESPONSIVNESS												
ADAPTABILITY	30.0	30.0	30.0	63.0	63.0	63.0	30.0	30.0	30.0	63.0	63.0	63.0
IMPLEMENTATION												
DELTA-COST	30.0	63.0	30.0	30.0	63.0	30.0	13.0	30.0	13.0	13.0	30.0	13.0
RISK												
TECHNICAL	63.0	63.0	63.0	63.0	63.0	63.0	63.0	63.0	63.0	63.0	63.0	63.0
SCHEDULE	50.0	50.0	50.0	50.0	50.0	50.0	75.0	75.0	75.0	75.0	75.0	75.0

Illustration 4-3. Raw Scores for System-Level Architectures with ST Agents

TYPE	ST AGENTS		VIP			
	YES	NO	TAC	ONE P	TAC + ONE P	TWO P
1	X		X			
2	X			X		
3	X				X	
4	X					X
5		X	X			
6		X		X		
7		X			X	
8		X				X

Illustration 4-2. Major Types of System-Level Architectures

To simplify the evaluation, the 48 candidate system-level architectures were grouped into eight major types as shown in Illustration 4-2. Illustrations 4-3 and 4-4 summarize the raw scores arrived at for these architectures (Type 1 through Type 8) and additional architectures resulting from the following combinations:

1. End-to-End security architecture used (involving IPLI and/or NET mode of STU-IIs)
2. Direct versus Behind-the-PBX interfacing.

Major additional considerations used in arriving at the raw scores are as follows.

1. For architectures employing the security architecture involving the IPLI _and_ NET mode of STU-II operation, the score is the highest (88) in Security criteria because of double encryption provided. Architectures employing the IPLI mode perform the worst in certification component of security criteria because IPLI is currently certified for use with data packets although it can be used with voice packets.
2. For architecture _with_ ST agents, the score is higher than the score for the _corresponding_ architectures _without_ ST agents in speed of service criteria because of ST agents implementation in the DDN PS nodes and gateways which provides a voice pipeline for voice packets in a call.
3. Architectures containing the Behind the PBX interfacing have a higher score in Adaptability criteria than those containing the Direct interfacing as a result of ease of expansion possible with the PBX (this possibly could be at the expense of increased call setup time).
4. Major factors used in Δ -Cost score of the architectures included hardware cost of external processor(s) (if used) and the S/S and Modem Modules in the VIUs; the software

4.3.2 Implementation

4.3.2.1 Implementation Strategy

The implementation strategy will depend on the final optimum architecture chosen for implementation after modeling and simulation and/or test-bed effort. The strategy must address three major catagories: hardware acquisition, software development, and transition and scheduling. It must also take into account the sound DoD systems engineering and acquisition practices.

As an example, consider the recommended architecture for the selected weight distribution. For this architecture, we recommend the following three-phase implementation strategy, (Illustration 4-11). The schedule shown in the Illustration meets the desired goal of implementing the secure voice, as provided by the STU-IIs, in the DDN I with minimum risk in the late 1980s time-frame.

Phase one consists of a clear definition of the functional requirements for the software system (including the recommended model of the protocol architecture) and for the hardware system (primarily the S/S and Modem Modules of the VIUs).

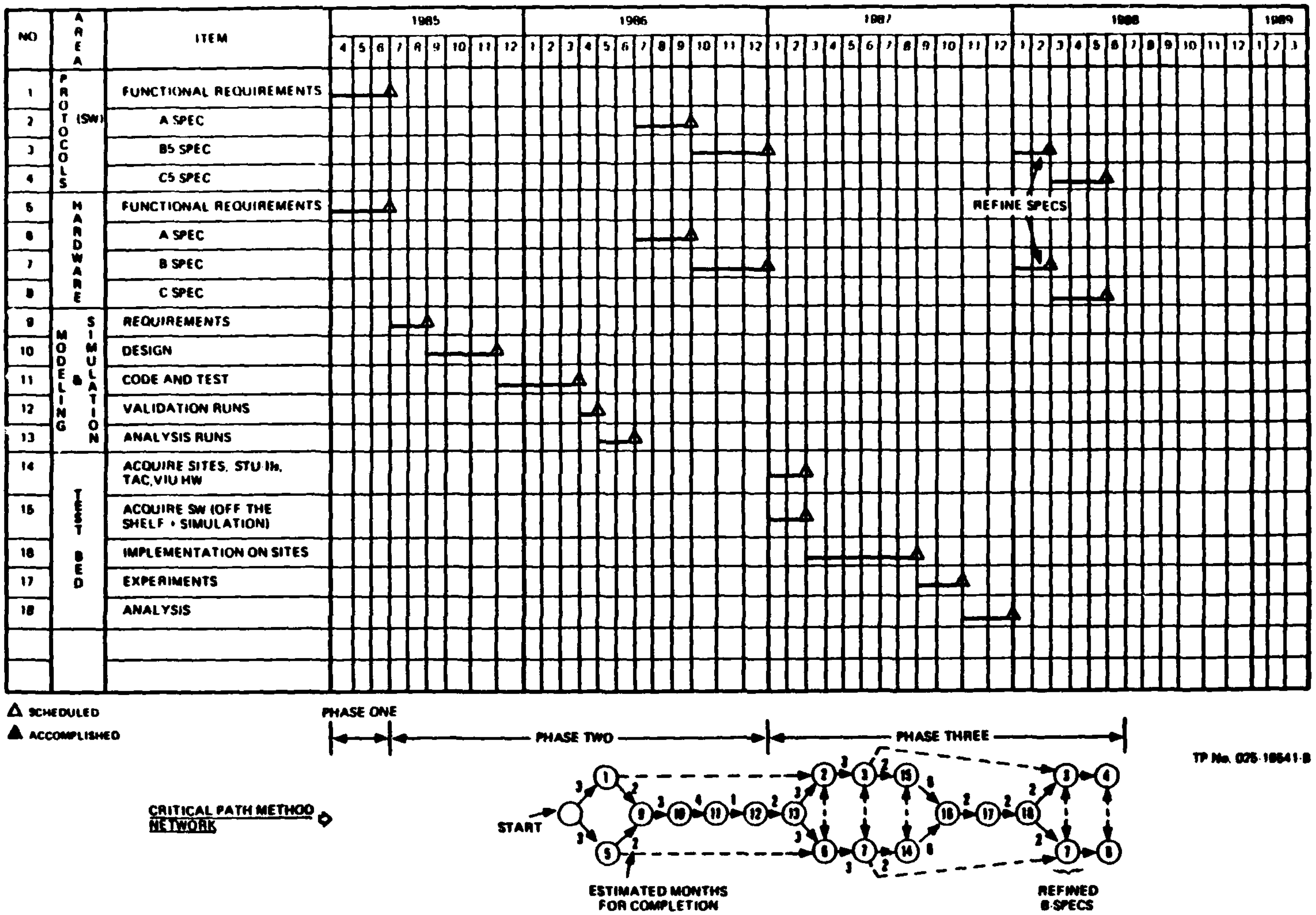
Based on these functional requirements software requirements for the modeling and simulation software can be developed in Phase two. Software requirements definition will be followed by the design, code and test (unit testing), and validation runs (system testing) components of the software development cycle before analysis runs can be conducted. The analysis runs will provide valuable performance data for A-level, and preliminary B-level specifications of the required hardware and software systems. Phase two will terminate at this point in time.

In order to validate the performance data in Phase two in a real-world environment, it is necessary to implement a test-bed, conduct experiments, and analyze the results of the experiments. This will be achieved in Phase three which will culminate in the refined B-level, and C-level specifications of the hardware and software systems. The test-bed in this phase will involve a

MAJOR MILESTONES

PROJECT TITLE IMPLEMENTATION PLAN FOR INCORPORATING STU IIs IN THE DDN I

REVISION NUMBER 0 DATE OF REVISION 2/19/85



NO	AREA	ITEM
1	PROTOCOLS (SW)	FUNCTIONAL REQUIREMENTS
2		A SPEC
3		B5 SPEC
4		C5 SPEC
5	HARDWARE	FUNCTIONAL REQUIREMENTS
6		A SPEC
7		B SPEC
8		C SPEC
9	MODELING & SIMULATION	REQUIREMENTS
10		DESIGN
11		CODE AND TEST
12		VALIDATION RUNS
13		ANALYSIS RUNS
14	TEST BED	ACQUIRE SITES, STU IIs, TAC, VIU HW
15		ACQUIRE SW (OFF THE SHELF + SIMULATION)
16		IMPLEMENTATION ON SITES
17		EXPERIMENTS
18		ANALYSIS

TP No. 025-18541-B

Illustration 4-11. Implementation Plan for Incorporating the Recommended System-Level Architecture in the DDN I selected DDN I backbone, the end sites (for the calling and called STU-IIs), acquistion of the necessary hardware (including TACs, S/S Modules, and Modem Modules) and software (including the protocol architecture software developed during the Phase two and the ST agents in the DDN I backbone), and implementation including hardware and software integration and test. Off-the-shelf hardware and software will be used to the maximum extent possible to minimize cost and reduce risk.

During all phases, standard practices in the DoD hardware acquisition (including specifications as per MIL-STD-490), new hardware development (if not off-the-shelf), and software development [Reference (3)] must be followed to the extent possible.

4.3.2.2 Δ-Cost for Implementing the Recommended System-Level Architecture

The following major considerations were employed in arriving at the Δ-cost for implementing the recommended system-level architecture to incorpore secure voice, as provided by the STU-IIs, in the DDN I in the late 1980s time-frame.

1. A three-phase approach as outlined in the above Paragraph will be used.

2. Cost of each S/S Module and Modem Module in the VIU is respectively $2,500. None of them can be shared by the STU-IIs.

3. One staff-month (SM) of contracted labor is roughly $8,334.

4. The calling and called STU-IIs (with PBXs), TACs, and the selected DDN I backbone are government furnished (GF).

5. Phase two cost is essentially the cost of implementing the recommended protocol architecture in the software. This amounts to roughly $281,000 (see Paragraph C.3 of Appendix C).

6. The ST agents software developed in the Phase two will be available and integrated in the PS nodes of the selected DDN I backbone at no cost.

Based on these considerations, the Δ - cost is as follows:

1.	Phase one -	$ 50,000
2.	Phase two -	$281,000
3.	Phase three -	$634,000
	Total for Three Phases =	$965,000

Thus, in order to incorporate the first calling STU-II to the called STU-II connection, for the selected system-level architecture, the Δ-cost is roughly $965K. The subsequent connections will require roughly $10K per connection, which is essentially the cost of the S/S and Modem Modules in the VIUs at the calling and called STU-II sites.

APPENDIX A

MILITARY NETWORK REQUIREMENTS

APPENDIX A - MILITARY NETWORK REQUIREMENTS

This appendix details the fundamental requirements on a military network to meet the worldwide survivability, security, performance, and responsiveness goals of the network users' missions or applications. References (1) and (14) are major sources for the details provided.

A.1 WORLDWIDE SURVIVABILITY

Network worldwide survivability is made up of three lower level components: invulnerability, measures on survivability, and restorability/reconstitution. Invulnerabiity is the degree to which the network is resistant to physical, electronic (jamming is an example), and nuclear threats (HEMP and radiation are examples). Measures on survivability include a ratio of service provided by the network under threat to that provided by undamaged network, and a percent of surviving critical user connections. The service provided is measured by call completion rate in voice applications and probability of correct message delivery in data applications. Restorability refers to the percent increase in network capacity from a minimum value (normally reached shortly after attack), assessed at predetermined times after the minimum is reached, as a result of control actions taken by surviving, in-place assets. Longer term improvements effected through repair or replacement of assets is defined as "reconstitution."

A.2 SECURITY

Network security implies security mechanisms or measures employed to protect the following major security concerns: passive intercept, active wiretapping, spoofing, traffic analysis, key protection, authentication control, logical and physical access control, and certification. Passive interception (monitoring or recording) of information bearing signals may occur on transmission links and (red) network nodes. Active wiretapping involves attachment of an unauthorized device to a communications circuit for the purpose of obtaining unauthorized access to data through the generation of false messages or control signals, or by altering the communications of authorized users. Spoofing is an act of inserting false or altered messages (using active wiretapping) with an intent to make it appear as valid at the receiving end or to cause denial of service. Traffic analysis involves analyzing passive intercepts leading to information on link volumes, link characteristics, and from-to distirubtions (revealing perhaps critical user connections). Key protection involves measures used in a network in key storage, loading, and transmission to deny enemy access to the key. Authentication control prevents imposters from using the network or its services (user authentication) and allows only valid messages to be processed in the network (message authentication). Unauthorized logical access may lead to an authorized user accessing information or resources for which the user has no access authorization or need-to-know. Association of security levels, compartments, and communities of interest are some of the techniques employed to enforce logical access control. Unauthorized physical access is an intruder entry of a secure perimeter in the network without authorization to gain classified (sensitive) information.

Without security mechanisms [link and end-to-end encryption, physical control zone (PCZ), and protected distribution system (PDS) are some examples] to protect the security concerns, security violations may occur in military networks resulting in one or more of unauthorized disclosure, modification, or destruction, or denial of service.

A.3 PERFORMANCE

Network performance can be grouped into two major catagories, timeliness and quality. In timeliness, parameters of major importance are call setup time (voice) and speed of service (packets, both voice and data). Call setup time is defined as the average time, over all calls, required to establish a call or circuit from the calling to the called party, measured from the last dialled digit (or its equivalent) to first ring received (or its equivalent). Speed of service is the average time, over all terminal pairs, a data transaction (packet and message are two examples) requires to move through the network measured from the first bit entered into the sending terminal to the last bit received at the receiving terminal. Quality parameters of major importance are intelligibility and naturalness (voice) and bit error rate (BER) (data). Intelligibility is the expected percent of speech transmitted over the network that will be correctly interpreted by the receiver. Naturalness is the degree to which the speech received over the network sounds like an unprocessed human voice in the absence of background noise. The BER is the average fraction of bits sent in a data transaction that are incorrectly received.

In military networks, usually the quantitative values of the timeliness and quality parameters are specified for user and/or functional missions. Timeliness is usually attained in the military networks, for critical missions, employing precedence/preemption techniques.

A.4 RESPONSIVENESS

Network responsiveness includes three major catagories: interoperability, adaptability, and ease of upgrade. Interoperability is the ability of the network to operate with other networks [United States (US) and allied, tactical, military, and commercial] based on some criteria. Adaptability implies ease of expansion, ease of extension/reconfiguration, and ease of reconstitution. Ease of expansion is a measure of increasing the capacity of the network without changing its connectivity. Ease of extension/reconfiguration is the ability of the network to accommodate changes arising from either extension of its geographical boundaries (to serve more users) or changes in netwcrk connectivity or transmission path (to serve the same set of users). Ease of reconstitution is the relative time required to restore a given percent of lost network capacity through repair or replacement of assets. Ease of upgrade is the inherent ability of a network to incorporate future technological changes at minimum cost.

In military networks, unlike in commercial networks, responsiveness is of critical importance particularly in times of stressed environments.

APPENDIX B

DDN I BASELINE ARCHITECTURE

APPENDIX B - DDN I BASELINE ARCHITECTURE

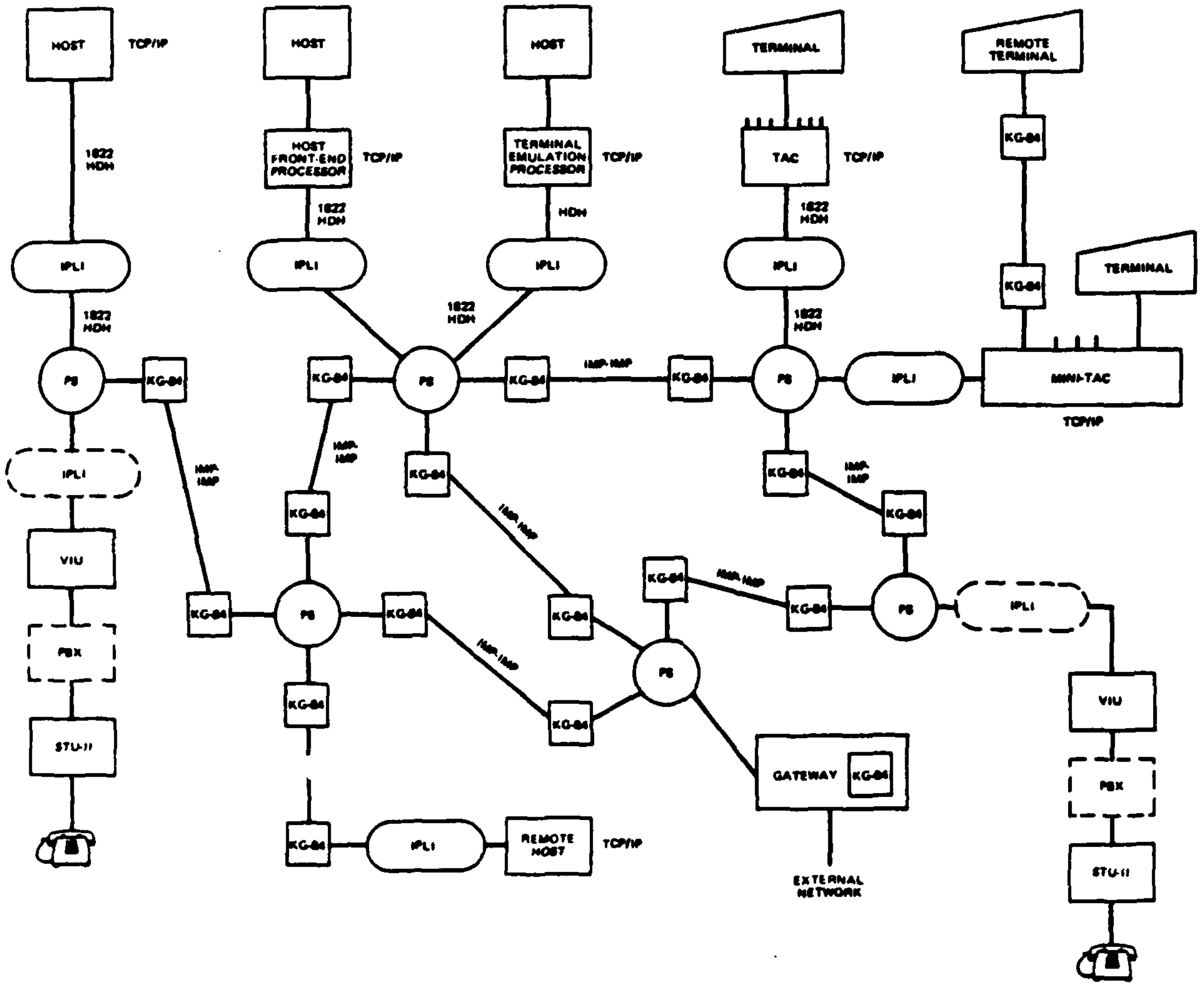
The DDN I baseline architectural features are described in this Appendix in terms of components used in three general catagories: network backbone, access area, and protocols. Illustration B-1 shows a simplified architecture of the DDN I (a proposed Voice Interface Unit (VIU) to incorporate STU-IIs to the DDN I is also shown) which is primarily derived from Reference (6), (15) and (16).

B.1 NETWORK BACKBONE COMPONENTS

Major network backbone components are packet switching (PS) nodes and backbone trunks.

The packet switching node will usually be a Bolt, Beranek, and Newman (BBN) C/30 packet switching processor in a TEMPEST/High-altitude Electromagnetic Pulse (HEMP) package. The C/30 hardware supports a full range of synchronous and asynchronous input/output (I/O) interfaces. The C/30s will support up to 80 full-duplex devices. There are two types of I/O boards that are used on DDN packet switches. For those hosts that support the 1822L protocol (provides physical and data link layer communications services between a packet switch and the attached device), an I/O board is available that allows packet switches to be up to 2000 feet from the host. For those hosts that support the HDLC protocol, an I/O board is available that allows a host to be at an unlimited distance from the packet switch. For an X.25 host connection to the packet switch, another I/O board may be required [(Reference (6)].

The C/30 software will be the ARPANET Interface Message Processor (IMP) program. The IMP software has four major functional capabilities:



TP No. 084-15022B

Illustration B-1. Simplified DDN I Architecture

1. Tandem (store and forward) traffic processing using an inter-node protocol

2. Host access and end-to-end traffic processing which offers both virtual circuit and datagram service, and a general logical addressing capability. The supported host access protocols include 1822 and X.25 protocols

3. Routing via a dynamic, adaptive, distributed routing algorithm

4. Monitoring and control services that provide status, alarms, fault isolation, diagnosis of hardware and software, and remote (downline) access for software maintenance.

Backbone trunks are used to connect PS nodes. They may use terrestrial and/or satellite communications circuits. Those trunk circuits requiring greatest capacity (highest speed) use common carrier dedicated circuits with transmission rates of from 19.2 Kbps to 56 Kbps (some dedicated, intra-site trunk circuits may use 230 Kbps cable circuits).

B.2 ACCESS AREA COMPONENTS

The access area components interface subscriber data terminals and host computers to the DDN. They include a Network Access Controller (NAC) and access links.

The NAC, which is a microcomputer based device, can be configured into one of the three major options: a mini-Terminal Access Controller (mini-TAC) or TAC, a Host Front End Processor (HFEP), and a Terminal Emulation Processor (TEP).

The Mini-TAC option supports communications between data terminals and remote hosts (but not terminal-to-terminal). Up to 16 terminal ports are available for the attachment of terminals, and two ports for interfacing to a network. Each terminal port is configurable as a synchronous or asynchronous port supporting erating characteristics which include half-or full-duplex eration; 75-9600 bits-per-second (bps) data rate (asynchronous) d up to 19200 bps data rate (synchronous); and ASCII, BCD, or CDIC characters. The network port interfaces to a PS node or an LI device and supports data rate of up to 56 Kbps.

The TAC prcvides terminal interface services similiar to the ni-TAC with some major differences: only asynchronous ports, up 56 Kbps data rate, and up to 63 ports. The TAC is one of the ındidates as the Voice Interface Processor (VIP) in the Voice ıterface Unit (VIU) which will be employed to interface the 'U-IIs to the DDN I.

The HEEP option supports communications between the attached ›sts and remote hosts and data terminals. The subscriber ports : the HEEP connecting one or two host, support operating ıaracteristics which include two-way simultaneous operation, data ıte of 4.8-56 Kbps, and transmission and receipt of binary igital data. The two ports of the HEEP on the network side have perating characteristics which include those on the subscriber ide. They interface to a PS node or an IPLI device.

The TEP option will interface a subscriber host to the DDN ia terminal ports on the host to support communications between ıe host and remote subscriber terminals (without disrupting the W or SW of the host or its communications front end). The TEP's erminal ports support operating characteristics which are upported on the terminal ports side of the mini-TAC. The two EP's network side ports interface to a PS node ›r an IPLI device nd support data rate of up to 56 Kbps.

One additional method of interfacinq a host computer to the)N exists. In this method (called Host Implementation), the host ill be connected to the DDN employing hardware interfaces which ›ntain no software. In this case the necessary supporting access rotocols are implemented in the host itself.

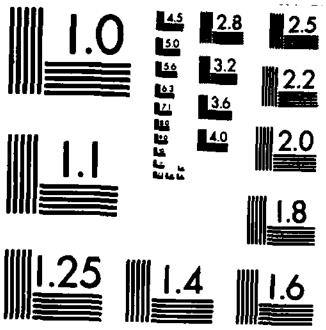
AD-A154 677 SECURE DIGITAL VOICE COMMUNICATIONS IN THE DEFENSE DATA NETWORK (DDN)(U) COMPUTER SCIENCES CORP FALLS CHURCH VA M BERNET ET AL. 15 MAR 85 DCA100-84-C-0030 2/2

UNCLASSIFIED F/G 17/2 NL

END

FILMED

DTIC



MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

Access links are usually dedicated circuits that connect remote subscriber devices to mini-TACs (or TACs) and PS nodes. Both the terrestrial and satellite facilities can be used as access circuits. Short end-to-end delay requirement may preclude the use of satellite facilities as access circuits in some instances (inter-active data traffic is an example). Trunk/access link speed combinations are planned for the DDN I with access link transmission rates of up to 19.2 Kbps. Access links for hosts can support link transmission rates of up to 56 Kbps.

B.3 PROTOCOLS

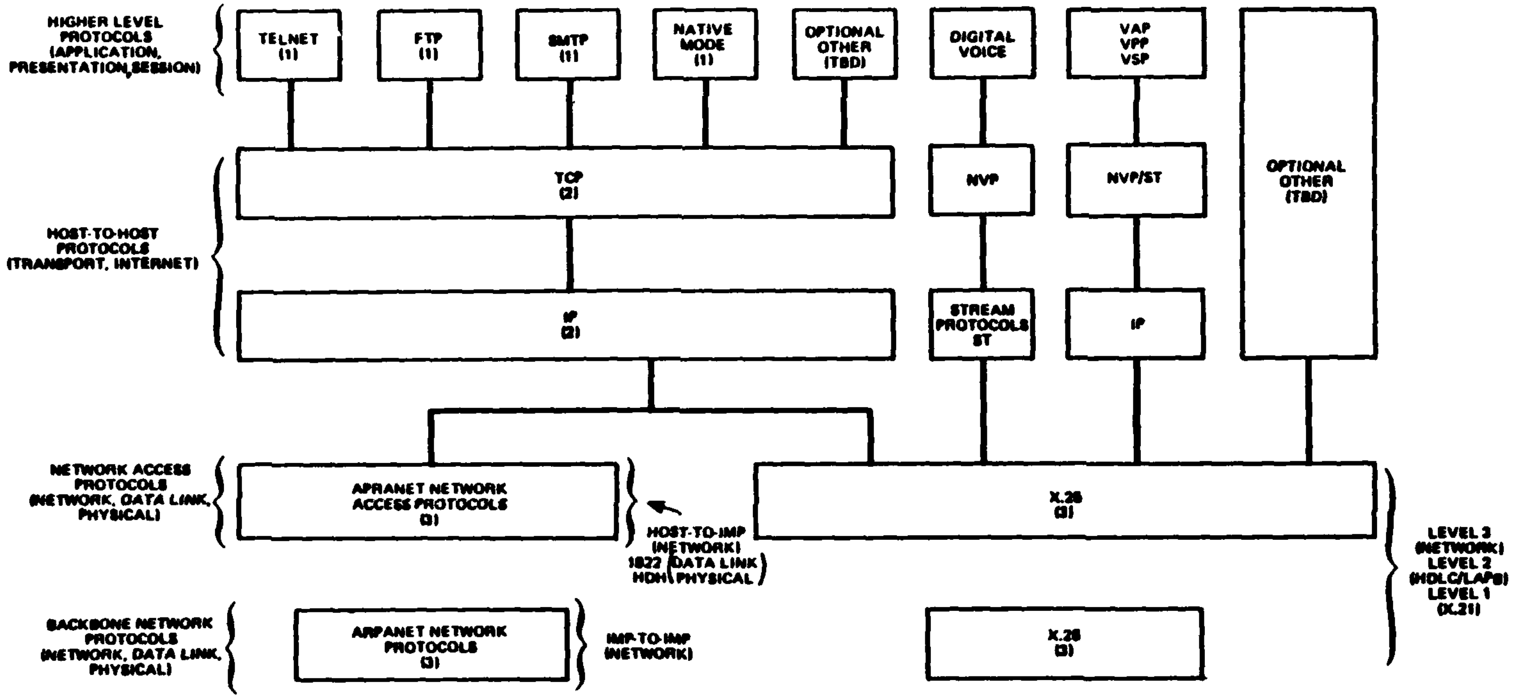
The DDN I protocols consist of four major groups: network backbone, network access, host-to-host, and higher level protocols as shown in Illustration B-2. They are summarized in the following.

B.3.1 Network Backbone Protocols

The backbone protocols are the ARPANET IMP-to-IMP protocol, routing update protocol, line up/down protocol, and end-to-end protocol. All are well documented in the public literature and have been running on the ARPANET for several years.

B.3.2 Network Access Protocols

The network access protocols define the interface between a subscriber device and the PS node. They encompass the physical, data link, and network levels of the Open Systems Interconnection (OSI) reference model. In the DDN either the ARPANET network access protocols or the X.25 protocols are mandatory as the network access protocols. The ARPANET network access protocol suite includes: 1822 protocol, HDLC Distant Host (HDH), and Very Distant Host (VDH). All of these use ARPANET Host-to-IMP protocol at network level.


HIGHER LEVEL PROTOCOLS (APPLICATION, PRESENTATION, SESSION)
TELNET (1)
FTP (1)
SMTP (1)
NATIVE MODE (1)
OPTIONAL OTHER (TBD)
DIGITAL VOICE
VAP VPP VSP
HOST-TO-HOST PROTOCOLS (TRANSPORT, INTERNET)
TCP (2)
NVP
NVP/ST
OPTIONAL OTHER (TBD)
IP (2)
STREAM PROTOCOLS ST
IP
NETWORK ACCESS PROTOCOLS (NETWORK, DATA LINK, PHYSICAL)
APRANET NETWORK ACCESS PROTOCOLS (3)
HOST-TO-IMP (NETWORK) 1822 HDH (DATA LINK PHYSICAL)
X.25 (3)
LEVEL 3 (NETWORK) LEVEL 2 (HDLC/LAPB) LEVEL 1 (X.21)
BACKBONE NETWORK PROTOCOLS (NETWORK, DATA LINK, PHYSICAL)
ARPANET NETWORK PROTOCOLS (3)
IMP-TO-IMP (NETWORK)
X.25 (3)

TP No. 084-18023-A

NOTES:
(1) RECOMMENDED FOR DDN HOSTS
(2) MANDATORY FOR DDN HOSTS
(3) ONE OF THESE IS MANDATORY

Illustration B-2. DDN I Protocol (Levels) Architecture

1. 1822 Protocol -The 1822 is an asynchronous, bit-serial interface providing physical and data link services over distances of less than 2,000 feet between a subscriber device and a PS node. The 1822 L (logical) protocol allows hosts to be addressed by a physical address (same as 1822) or by a physical location independent logical address. See Reference (4) for details of 1822 and 1822L.

2. HDH Protocol - The HDH protocol uses the standard HDLC protocol at the link level (LAPB), HDH encapsulation and line monitoring, and the standard physical level interfaces (RS-232, RS-422 are examples). It will service distances greater than 2,000 feet between a subscriber device and a PS node [see Reference (4)].

3. VDH Protocol - The VDH protocol is a predecessor of the HDH protocol supporting non-standard physical and link level protocols for use with many existing systems. It will not be generally used in the DDN I.

4. X.25 - The X.25 is the standard network access protocol as recommended by CCITT and DCA [see References (5) and (6) respectively]. The C/30 PS nodes supports all three levels; physical, data link, and network of the X.25.

B.3.2 Host-to-Host Protocols

Hosts which connect to the DDN I will have two fundamental choices for host level end-to-end protocols: DoD standard Transmission Control Protocol/Internet Protocol (TCP/IP) or their own special protocol. The use of TCP/IP is mandatory in the DDN unless it is demonstrated there is no requirement for interoperability and a waiver is granted. The TCP/IP protocols, which provide reliable host-to-host peer level communication, can be implemented either in the host themselves, or in front-end processors. Many TCP/IP implementations are currently in use on the ARPANET.

1. Internet Protocol (IP) - The IP is designed to support transmission of data across multiple, interconnect PS data communications networks (a CATENET environment). It resides in the internet level and is used in conjunction with the TCP transport level. Typically the IP supports datagram service and provides for fragmentation and reassembly of large datagrams that transmit "small packet size" network [see Reference (7) for details]. The IP has been retained for use with the voice packet transmission.

2. Transmission Control Protocol (TCP) - The TCP is a transport level protocol which provides for reliable, end-to-end communications needed to operate the possibly less unreliable lower level service (IP datagram is an example). The TCP accomplishes this by using virtual circuits, sequencing, and positive acknowledgements (ACK) mechanism [see Reference (8) for details]. The TCP will not be used with the voice packets.

B.3.3 Higher Level Protocols

Higher Level protocols to be supported in the DDN for data applications include TELNET protocol, File Transfer Protocol (FTP), and Simplified Mail Transfer Protocol (SMTP).

The TELNET protocol provides communications between data terminals and remote hosts across a network. Data terminals which use TELNET can communicate with dissimiliar terminals by the use of a Network Virtual Terminal (NVT) mechanism. TELNET requires the services of TCP or similiar protocol; in practice TCP must be implemented to support TELNET implementation [see Reference (9) for details].

The FTP supports the transfer of data files among network hosts and provides access to file manipulation function [see Reference (10) for details]. The SMTP supports the reliable and efficient transfer of electronic mail over the DDN [see Reference (11) for details]. As in the TELNET, TCP usually must be implemented to support both the FTP and SMTP.

Continuing research activity in the higher level protocol area has resulted in two protcols, Network Voice Protocol (NVP) [Reference (12) and Stream (ST) protocol [Reference (13)] suitable for use with voice packets in a PS network. The ST protocol supports both the point-to-point and conference type voice connections. The ST protocol at the internet level in conjunction with the NVP protocol at the transport level supports voice connections.

The protocol suite we have developed in this investigation to incorporate STU-IIs in the DDN I, consists of VAP, VPP, VSP as higher level protocols; NVP/ST and IP as host-to-host protocols; and DDN X.25 network access protocols (Illustration B-2). The higher level and host-to-host protocols are based on the NVP and ST protocols with necessary modifications including those which are required to support security feature of the secure voice. See Appendix C for details on the protocol suite.

APPENDIX C

IMPLEMENTATION MODEL OF PROTOCOL ARCHITECTURE TO SUPPORT SECURE DIGITAL VOICE IN THE DEFENSE DATA NETWORK (DDN)

APPENDIX C - IMPLEMENTATION MODEL OF PROTOCOL ARCHITECTURE TO SUPPORT SECURE DIGITAL VOICE IN THE DEFENSE DATA NETWORK (DDN)

C.1 BACKGROUND, PURPOSE, SCOPE, AND ORGANIZATION

C.1.1 Background

C.1.1.1 General Requirements

General Requirements to support secure digital voice in the DDN I are stated in Illustrations 2-2 and 2-3 of Section 2. A subset of these requirements will be satisfied by the proposed implementation model of the protocol architecture as described in the following paragraphs.

C.1.1.2 Requirements Supported by the Proposed Model of the Protocol Architecture

The proposed model of the protocol architecture will provide for: negotiations and appropriate signal generation for call initiation and termination and connection setup, optimized voice packet size, voice packet transmission, buffering, packet assembly and disassembly, and speech reconstitution supporting the STU-II speech synthesis.

Near real-time speech delivery of voice packets will be achieved by assigning precedence to voice packets, minimizing overhead, eliminating end-to-end acknowledgment for voice packet transmission, but not for control messages, and using stream (ST) agents in the DDN I packet switched (PS) nodes and gateways. Finally local and remote interoperability, simultaneous users, and cryptosynchronization will be satisfed by the protocol architecture.

C.1.2 Purpose and Scope

The purpose of proposed model of the protocol architecture is to support the incorporation of secure voice as provided by the STU-II family of secure voice terminals in the DDN I. The proposed model of the protocol architecture will satisfy the stated requirements within the late 1980s time-frame implementation of the DDN (DDN I) and is flexible enough to be expanded for the 1990s time-frame implementation of the DDN (DDN II).

The protocol architecture will make use of standard, existing, and planned protocols to the maximum degree possible. Modifications will be introduced into these protocols, or new protocols added, only when it is necessary.

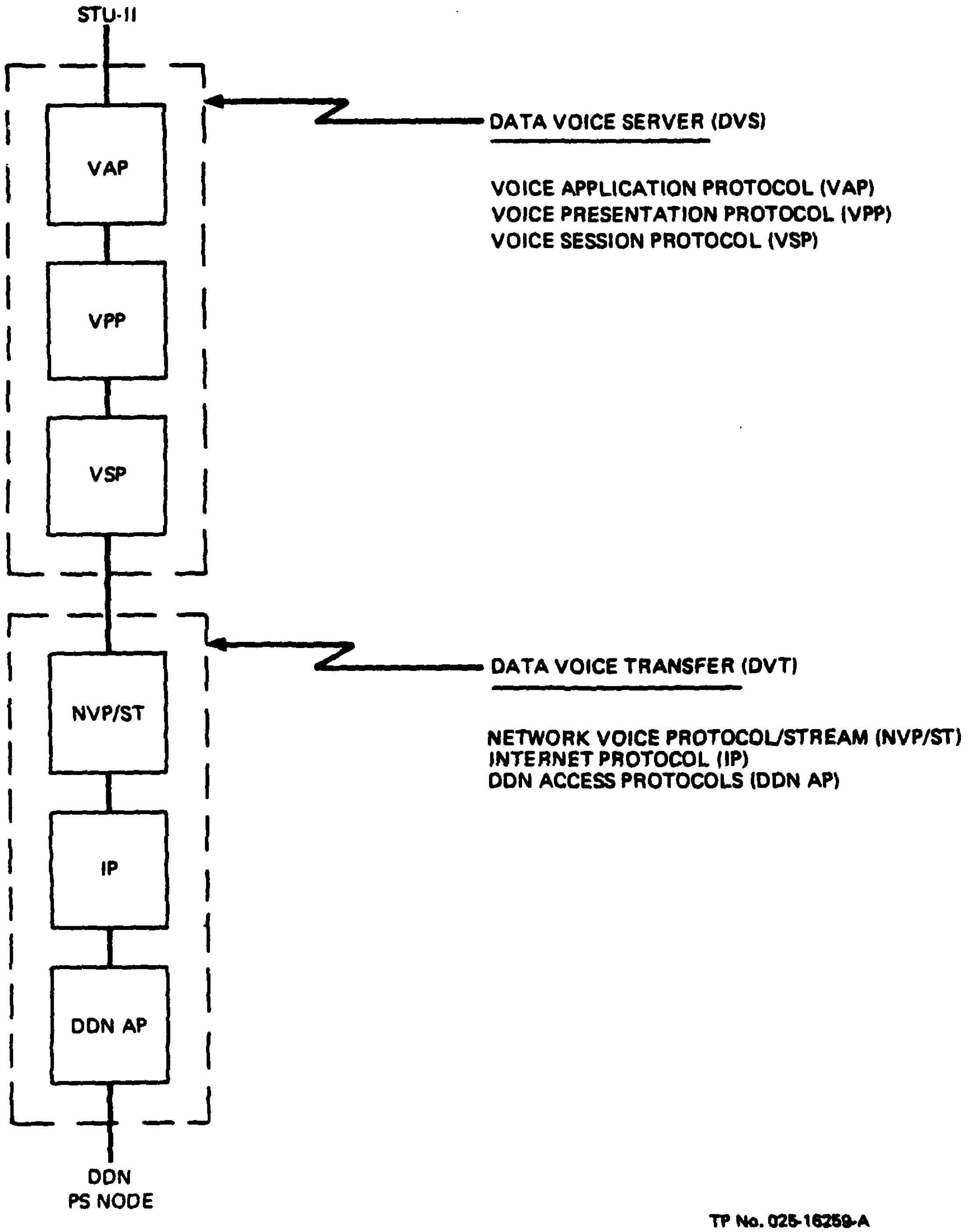
C.1.3 Organization

Paragraph C.2 details the proposed model of the protocol architecture. Protocol implementation considerations including hardware and software cost is contained in Paragraph C.3. How the protocol architecture supports various scenarios is described in Paragraph C.4. A concise summary of the Appendix is provided in Paragraph C.5.

C.2 PROPOSED MODEL OF THE PROTOCOL ARCHITECTURE

The proposed model of the protocol architecture for digital secure voice is shown in Illustration C-1. It consists of seven protocol layers grouped into two functions: Data Voice Server (DVS), and Data Voice Transfer (DVT).

The DVS defines the functions directly following the STU-IIs. It acts on behalf of a STU-II and assists in preparing buffering, sending, and receiving digitized voice, STU-II signals, and STU-II control messages. The DVS consists of Voice Application Protocol (VAP), Voice Presentation Protocol (VPP), and Voice Session Protocol (VSP), which are respectively detailed in Paragraph C.2.1 through C.2.3. These protocols correspond to the three higher-level protocols recommended by International Standards Organization Open System Interconnection Reference Model (ISO OSI/RM) in their protocol reference guide [Reference (21), and are primarily based on the planned NVP protocol [Reference (12)].


STU-II
VAP
VPP
VSP
NVP/ST
IP
DDN AP
DDN
PS NODE
DATA VOICE SERVER (DVS)
VOICE APPLICATION PROTOCOL (VAP)
VOICE PRESENTATION PROTOCOL (VPP)
VOICE SESSION PROTOCOL (VSP)
DATA VOICE TRANSFER (DVT)
NETWORK VOICE PROTOCOL/STREAM (NVP/ST)
INTERNET PROTOCOL (IP)
DDN ACCESS PROTOCOLS (DDN AP)

TP No. 025-16259-A

Illustration C-1. Proposed Model of the Protocol Architecture for Digital Secure Voice

The DVT contains two sets of protocols: the transport protocols and the network access protocols. The transport protocols are the Network Voice Protocol/Stream (NVP/ST) and the Internet Protocol (IP). The NVP/ST is based on the planned ST protocol [Reference (13)] with certain modifications explained in Paragraph C.2.4. The IP (Paragraph C.2.5) is the standard internet protocol for CATENET environment [Reference (7)]. The network access protocols (Paragraph C.2.6) are the X.25 recommendation [Reference (5)] in its three levels, the X.25 level 3, the High-level Data Link Control (HDLC) LAPB, and the physical level interface protocol, typically X.21B.

A functional view of the DVS and DVT in the DDN I is shown in Illustration C-2. Illustration C-3 summarizes the mapping of the new protocols within the proposed protocol architecture, into the planned protocols.

In the following the individual protocols within the DVS and DVT are detailed in terms of their functions and services, the message formats used, and interfaces.

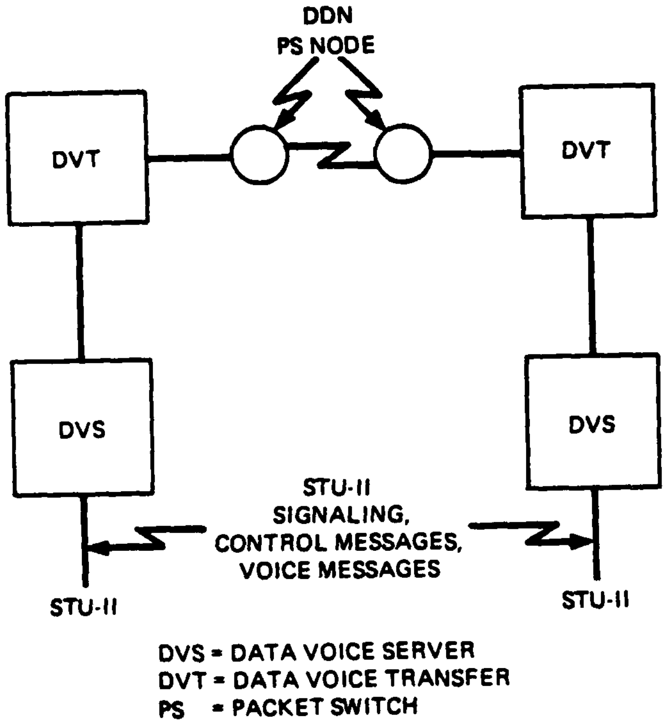


Illustration C-2. Functional View of the DVS and DVT in DDN I

New Proposed Protocols		Current/Planned DoD Protocols
VAP	Based on	Control Segment of Network Voice Protocol (NVP**), proposed in Reference (12) by Danny Cohen
(VAP requires about 30% work in requirements and design areas and 100% work in implementation)		
VPP	Based on	Data Segment of the NVP***
VSP is a new protocol		
NVP/ST*	Based on	Internet Stream (ST) Protocol, proposed in Reference (13) by James W. Forgie
(NVP/ST requires about 10% work in requirements, 10% work in design, and 100% work in implementation areas)		

Note: * NVP/ST is the new proposed protocol for voice transport based on the ST protocol. It has no relationship to the NVP**

Illustration C-3. Mapping of New Proposed, Protocols into the Current/Planned DoD Protocols

.2.1 Voice Application Protocol (VAP)

.2.1.1 VAP Functions and Services

The VAP is based on the NVP control segment [Reference (12)].

The VAP is activated as soon as the OFF-HOOK state of the TU-II handset is detected via the OFF-HOOK signal received.

The VAP will accept the STU-II control messages, digital peech and STU-II signaling and supervision (S/S). A STU-II can nitiate an encrypted (secure or black) or unencrypted (clear) onnection. Whether the required connection is secure or clear, he STU-II control messages, exchanged between calling and called TU-IIs before the GO SECURE message is issued, are always in the lear. Once crytosynchronization or sync has been achieved, igital speech processed, will be encrypted.

The dialed numbers in the S/S, received via Dual Pulse or TMF signals, are converted to suitable network addresses. The ialed number will have an International Code Number (Country and ity), or an area code number plus local number, or local number s destination address depending upon where the call is to be nade. The address is structured to identify the recipient within the originating server's local link or when attached to any etwork, within the subscriber domain.

A precedence field, which is activated by the STU-II user, will be used by the VAP to indicate priority calls to the called TU-II.

The functions supported by the VAP include:

1. Call initiation (including dialed number to DDN I network address translation)
2. Handling of ringing and busy conditions
3. Call termination
4. Digital speech frames assembly into voice packets

intermediate ST agents if they are unable to support the connection requested. An ST agent receiving such a REFUSE attempts alternate routing, and sends the REFUSE back one hop only after exhausting all other alternatives. REASON codes are included in the REFUSE command. The ACCEPT and CONNECT command contains the same information, except for the CID and FLOW-SPEC which change from hop-to-hop.

If the ST agents were not present, the IP will get the source and destination addresses and parameters from the NVP/ST interface, and the packets are transfered from the ORIGIN to TARGET by the IP. The FLOW-SPEC and CID have no effect. Taking a connection down is initiated either by an ORIGIN issuing a DISCONNECT message or a TARGET issuing a REFUSE message. The intermediate ST agents will then delete their stored information about the connection.

Connections can also be taken down as a result of a faulty link or gateway. In this case an intermediate ST agent will issue a DISCONNECT/REFUSE pair. A REASON code is included in the messages.

FLOW-SPEC is carried out by the CONNECT and ACCEPT messages, and contains many fields. Data rate and flow type parameters are specified in these fields. These fields also include a ROUTING-STRATEGY parameter.

C.2.4.2 NVP/ST Message Formats

The NVP/ST packet is designed to have an abbreviated header to improve packet transmission efficiency. When the ST agents are present, header information will change on a hop-to-hop basis as the packet travels from one ST agent to another. The packets are buffered for a short time only and are discarded by the intermediate ST agents if queueing conditions show long delays. In the first case, with no ST agents present, the IP will deal with the packets as standard datagrams. Voice packets will not be retransmitted, therefore no error detection and correction

The NVP/ST could service both point-to-point (PTP) and conference connections. Only the PTP connections are discussed in this investigation. The PTP connections are set up in response to a CONNECT command from an originating process (NVP/ST) to an ST agent. It will begin the negotiations for the establishment of the connection. The CONNECT specifies the following:

1. The NAME of the connection. This provides the originating internet host address and the process in the host. It is the responsibility of the originating process (NVP/ST) to provide the NAME

2. The internet address of the process to which the connection is desired. This address is called the "TARGET"

* 3. A flow specification (FLOW-SPEC) that tells the ST agent about the data rate requirement and a precedence value, if used, for incorporation in the flow control strategy

* 4. An arbitrary 16-bit number that the agent is to use to identify the connection [connection ID (CID)] for sending all the NVP/ST packets in the call. CID.B is used to identify packets sent in the backward direction, and CID.F for packets sent in the forward direction. The CID will change on a hop-to-hop basis, since it is unique to each agent.

Note: * Will not be possible without the ST agents.

The CONNECT command propagates from an ST agent to an ST agent until it reaches its TARGET process. The intermediate ST agents inspect the command, take appropriate action, and retain information about the requested connection. If the TARGET agrees on the connection, it sends an ACCEPT command that propagates back to the originator through the same ST agents. If the TARGET process is not willing to accept the connection, it sends back a REFUSE command on the same path. REFUSEs are also generated by the delay for the offered stream. They will also use a distributed routing algorithm in finding a route with sufficient capacity. This will usually result in fixed-path internet route. In the case of failure of a PS node or gateway, automatic rerouting will be provided by the ST agents. The agents will retain information about the connections to help detect faults. The agents will also provide flow control and delay and data rate management. The IP will still be used so that the gateways, which do not support ST agents, can be used. The ST agents will just ignore the IP header, and get to the NVP/ST header. In the first case, all the information pertaining to the ST agents will simply be ignored, but will remain for future use.

The NVP/ST is required to provide guaranteed data rates and controlled delay needed for packet voice communications. It will also support an efficient and sequential delivery of voice packets. The NVP/ST provides low delay characteristics and low delay dispersion to maintain speech intellegibility and naturalness. Voice packets delayed beyond a certain limit will be discarded, however, the loss of packets should be kept to a minimum. The loss of small chunks of speech (50 msec or less) will produce degradation in voice quality but will preserve sentence intelligibility. The probability of loss should be kept at 1% or less. Obviously, delay and data rate achievements depend on the network too, therefore, the network is required to offer some help, for example, by throttling unoperative users and avoiding slow routes.

Full-duplex connections are used, but the connection has an orientation. Packets are said to move in the "forward" direction if they are moving away from the originator (calling STU-II), and in the "backward" direction if they are moving toward the originator.

translate the NVP/ST header, and provide the user with all the NVP/ST characteristics, guaranteed data rate and delay control, and an efficient delivery of packets. The NVP/ST has been designed to take into account this restriction and possible changes in the future as outlined below under two cases.

The first case is the presently planned DDN I. The DDN I does not have ST agents in the PS nodes (and gateways) and therefore does not support the NVP/ST. This will mean that the standard Internet Protocol (IP) has to be used for the transport services. The NVP/ST will perform connection setup negotiation on a peer level, while the actual packet transport will be done by the IP. The NVP/ST packet will be embedded in the IP datagram, and will be treated as normal IP data. This, of course, will strip the protocol of its routing and data transfer characteristics, and will introduce inefficiencies due to the possibility of the data being lost or delayed, or arriving out of sequence. The NVP/ST, in order to minimize buffering delays as much as possible, will introduce, through IP and X.25 interface, precedence bits which will indicate that the data packet contains voice, and should be given priority. Additionally, when the network reaches its local load-limit, the NVP/ST will reject (or hold off) new offered load on a call basis, and not on an individual packet basis. Thus voice packets in calls already in progress will be allowed in the network.

The second case will occur when the DDN switch software (PS nodes and gateways) is modified to include ST agents. This will mean that the network can now support the NVP/ST. This will not require any change in the NVP/ST since it is designed for use with the ST agents. The ST agents will be able to make use of the information in the NVP/ST headers that was ignored in the first case. The ST agents will then be able to participate in the local data management. The agents will determine whether or not resources are available to support the required data rate and

C.2.3.3 VSP Interfaces

The VSP interfaces with the VPP and NVP/ST. The interface between these protocol layers is realized by processing commands, responses, and messages.

The first call the VSP receives from the VPP is a command to open a connection providing source and destination addresses. The VSP will then call the NVP/ST requesting a connection passing the source and destination addresses received from the VPP. All lower level protocols (to the VSP) will process the open request. After the connection is established the NVP/ST returns to the VSP with the open ID. The VSP stores the open ID in the assigned location of the header and transmits its [open] command message to its VSP counterpart at the destination server through its just established link. Once the acknowledgment is received, the VSP returns to the VPP passing back the open ID.

The close request is handled in the same manner as previously described for the VAP and VPP. That is both the VSP peer-protocols negotiate the close, sending a [close] control message, and receiving a [close] response control message. Once this exchange is completed the VSP calls the NVP/ST requesting the close of the connection.

C.2.4 The Network Voice Protocol and Stream (NVP/ST) Protocol

C.2.4.1 NVP/ST Functions and Services

The NVP/ST is required to provide all the data transfer characteristics needed for packet voice communications. It is based on the internet Stream (ST) Protocol [Reference (13)] with modifications to accomodate the restrictions imposed by the DDN.

The restriction on the NVP/ST, and thus on the efficiency of voice communications, is the absence of ST agents from the DDN I switch software. These agents when present, will be able to management of data messages (including speech) will consist of sending the messages to the next protocol layer as soon as they are received to support near real-time speech delivery. No end-to-end acknowledgment is required, no end-to-end acknowledgement is awaited.

C.2.3.2 VSP Message Format

The VSP employs both control and data messages. The control message will have the format as shown in Illustration C-8.

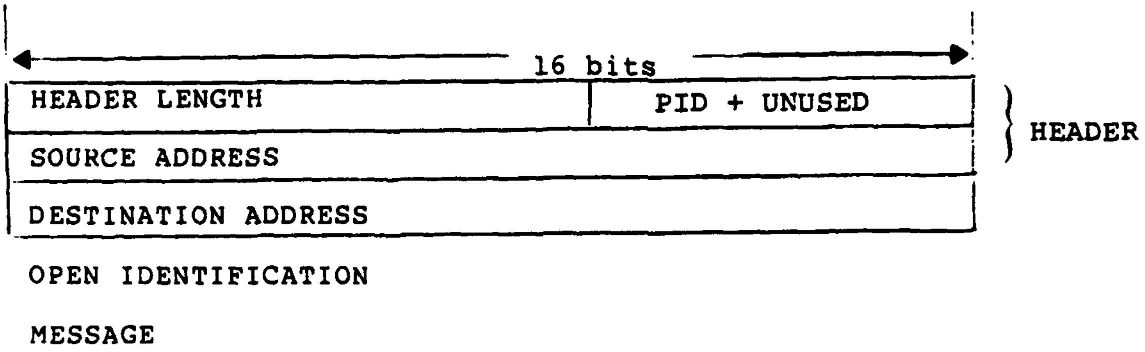


Illustration C-8. VSP Control Message Format

The control functions are those required to establish the connection. Once the session connection is established, data can be sent and received at this level.

The data (including speech) messages will have the format shown in Illustration C-9.

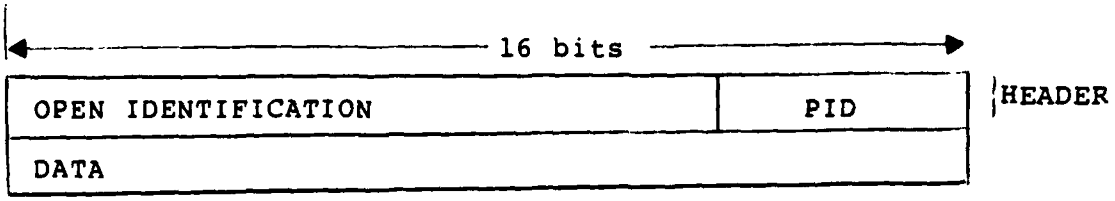


Illustration C-9. VSP Data Message Format

The first call the VPP receives from the VAP is a command to open a connection providing source and destination addresses. The VPP protocol will proceed in two steps: first it will prepare an [open] control message for its peer-protocol at the destination end, and second it will call the VSP requesting a connection.

After all the lower level protocols have processed the [open] control message, the VSP returns to the VPP with the same open ID. The VPP will store this in the header of its [open] command message and send it through its just established link. A positive acknowledgement from its peer protocol will trigger its return to the calling VAP passing back the open to it.

The close request is handled by the VPP in the same manner as described for the VAP. A [close] control message is sent to its destination peer-protocol and after receiving an acknowledgment, the VPP calls the VSP with a close request.

C.2.3 Voice Session Protocol (VSP)

C.2.3.1 VSP Functions and Services

The purpose of the VSP is to provide both administrative and connection services.

The administrative services consist of gathering connection statistics such as call setup time, establishment of the local link with the destination VSP, activation of the appropriate user processes, and session authorization.

The connection services consist of control messages and management of data messages. The control messages include as a minimum the open and close commands, and their corresponding responses. A control message, requires a response before any other control message is sent. This means that an explicit acknowledgement is required. The VSP will also manage the alternation of responses and requests, making sure that the responses are in the same sequence as their requests. The

The SOURCE ADDRESS is the calling address. The DESTINATION ADDRESS is the called address.

HEADER LENGTH contains length of the header in words. MESSAGE will contain the control parameters used in negotiations.

The MESSAGE types include:

1. Negotiation inquiry (specifying information enquired)
2. Positive negotiation response
3. Negative negotiation response (specifies options for enquiring)
4. Renegotiation request. Request to change negotiation master
5. Renegotiation approval. Approve the request.

The data message will have the format given in Illustration C-7.

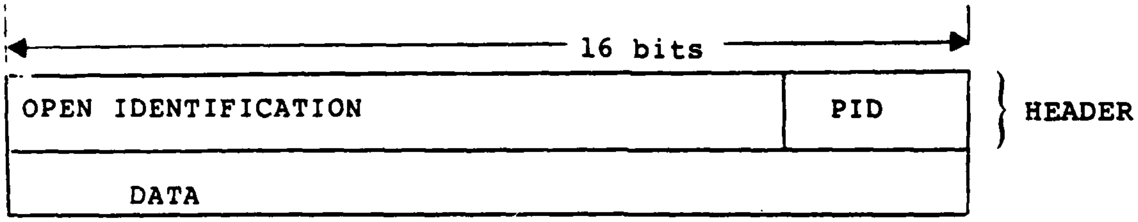


Illustration C-7. VPP Data Message Format

OPEN IDENTIFICATION: Replaces source and destination addresses for this connection

DATA: Control or speech message from upper protocol layer

C.2.2.3 VPP Interfaces

The VPP interfaces with the application (VAP) and session (VSP) protocols. The interface between these protocol layers is realized passing commands, responses, and messages. Tne interface between pair-peer protocols is attained passing control messages and data (speech) messages.

C.2.2 The Voice Presentation Protocol (VPP)

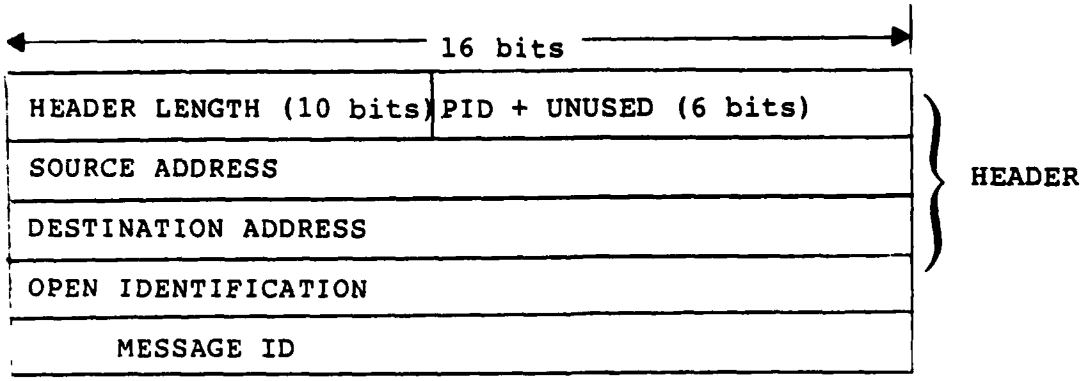
C.2.2.1 VPP Functions and Services

The VPP provides for negotiations between the calling and called STU-IIs (if needed) to establish common physical characteristics and data message exchange compatibilities. A connect request is negotiated between the calling and the called VPP, and will result in either an acceptance or rejection of the request. Detailed negotiations are described in the Reference (12) which is the basis for the VPP. Negotiated items include sampling period, coding schemes and different options, status enquiries, and choice of either encrypted or unencrypted speech.

C.2.2.2 VPP Message Formats

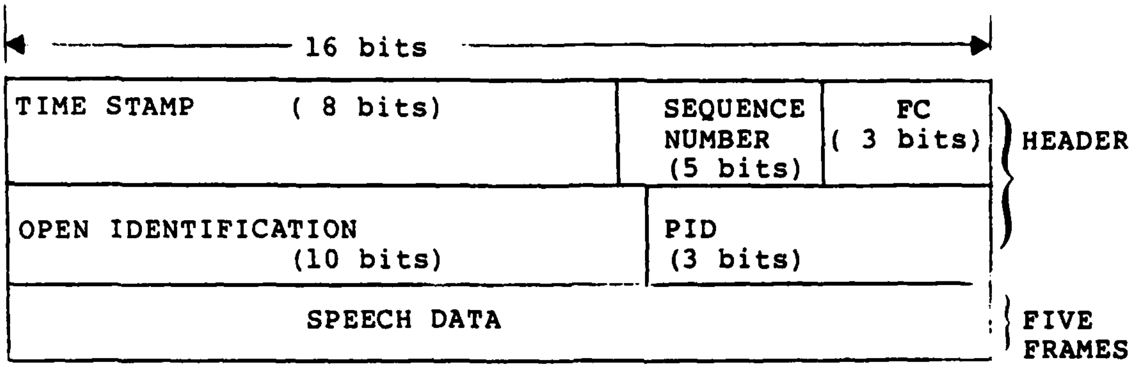
The VPP generates both control and data messages.

The control message format is shown in Illustration C-6.



HEADER LENGTH (10 bits)	PID + UNUSED (6 bits)
SOURCE ADDRESS	
DESTINATION ADDRESS	
OPEN IDENTIFICATION	
MESSAGE ID	

Illustration C-6. VPP Control Message



TIME STAMP = One time stamp is assigned to each voice packet

SEQUENCE NUMBER = Number assigned incrementally to voice packets in a talkspurt

(Note: TIME STAMP in conjunction with SEQUENCE NUMBER provide a complete and unique identification to voice packets in a talkspurt)

FC = Frame Counter - Used to indicate the number of voice frames contained in that voice packet since a voice packet may not always contain five voice frames

OPEN IDENTIFICATION = Assigned to the link replacing source and destination addresses in the message, thus minimizing leader length/overhead

PID = Identifies protocol and type of message

Illustration C-5. VAP Speech Message Format

Upon completion of the initial phase of the connection and after successful negotiations, a unique open identification is assigned for the connection on these links. The speech message, transmitted on the links, will have the format shown in Illustration C-5.

C.2.1.3 VAP Interfaces

The VAP directly interfaces with the STU-IIs, and must be able to accept all messages, data and commands. The output message from the VAP is passed to the Voice Presentation Protocol (VPP). The message will traverse all protocol layers in the VIP and navigate through the DDN until received by its peer VAP at the destination VIP.

Incoming messages from remote STU-IIs will be stored using multibuffering techniques. While one packet is being disassembled, packets are received and stored three per buffer.

When openning a connection the VAP formats its open command and issues a call to the VPP passing as parameters the source and destination addresses and the [open] request. After, all the lower protocols have processed the OPEN, VPP returns to VAP with an open identification or a connection denial.

The VAP stores the open ID and sends its open control message through the lower layer protocols to its peer VAP protocol at the destination server, and waits for a control response. A ready will acknowledge the establishment of the connection with its VAP counterpart.

When closing a connection the VAP layer sends the close command to its peer protocol at the destination server, and waits for the acknowledgment. Once received, it calls the VPP with a [close] command.

Ringing is sent by the called STU-II after the negotiations, if used, have been successfully completed. Echo is used in measuring the network delays.

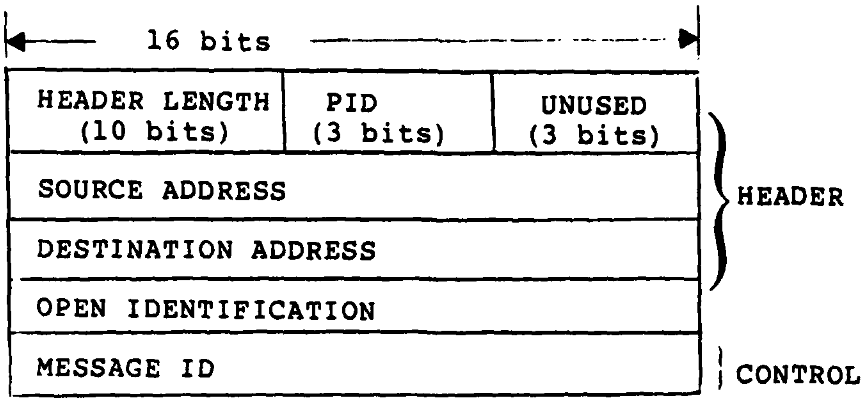


Illustration C-4. VAP Control Message Format

The 10 bit header length, which contains the length of HEADER in words, points to the control message (MESSAGE ID) and PID is the protocol identifier (3 bits). The SOURCE ADDRESS is 16 bits long (HHHIIIIIIXXXXXXX) and identifies the call originator (calling STU-II). The DESTINATION ADDRESS identifies call recipient (called STU-II) and is also 16 bits long (HHHIIIIIIXXXXXXX).

HHH: identifies Host (Processor Module in the VIU)

IIIIII: identifies IMP

XXXXXXX: identifies a host extension (STU-IIs connected to a VIU)

The OPEN IDENTIFICATION (ID) provides an area to store the identification received when the open connection has been established. The calling [open] control message is issued first on a link (say 377). The message will identify the calling and called STU-IIs and a link (say K) for the called STU-II response. The called STU-II either refuses the call or accepts it and assigns link L for the calling STU-II. All further transfers from the calling STU-II to the called STU-II are done on Link L.

store five voice frames at 2.4 Kbps Voice Digitization Rate (VDR). A frame count field will be included in each packet to allow for a variation in the n..ber of voice frames per packet. A time stamp and sequence number will be attached to each voice packet. A timeout interval of 200 msec will be maintained at the call orignating VAP for a nominal network delay. This will mean that the packet is closed when the time difference between two successive voice frames is larger than 200 msec. The next arriving voice frame from the calling STU-II will then be placed in the next available buffer for assemby in the subsequent packet.

Third, voice packets transported through the network can tolerate on average, 377 msec of delay without degrading the received voice quality. This corresponds to about 906 bits at 2.4 Kbps transmission rate or three voice packets, since at the VAP the voice packet size is 302 bits including the VAP overhead of 32 bits. Therefore, the output buffer size is selected to contain three voice packets.

The reconstitution algorithm has to buffer the incoming voice packets, disassemble the voice frames, and decide when to play them out based on the time-stamp information. It will also identify missing or out-of-sequence packets and ensure that a continuous string of bits is sent (bit count integrity) to the called STU-II to ensure that the calling and called STU-IIs keep in synch during encrypted sessions when the NET mode of STU-IIs is employed for end-to-end security.

C.2.1.2 VAP Message Formats

The VAP will employ two types of messages: control and speech.

The control message format is shown in Illustration C-4. The set of control messages will include: Calling [Open], goodbye [close], and their respective responses; ready, not ready, I am busy, ringing, and echo.

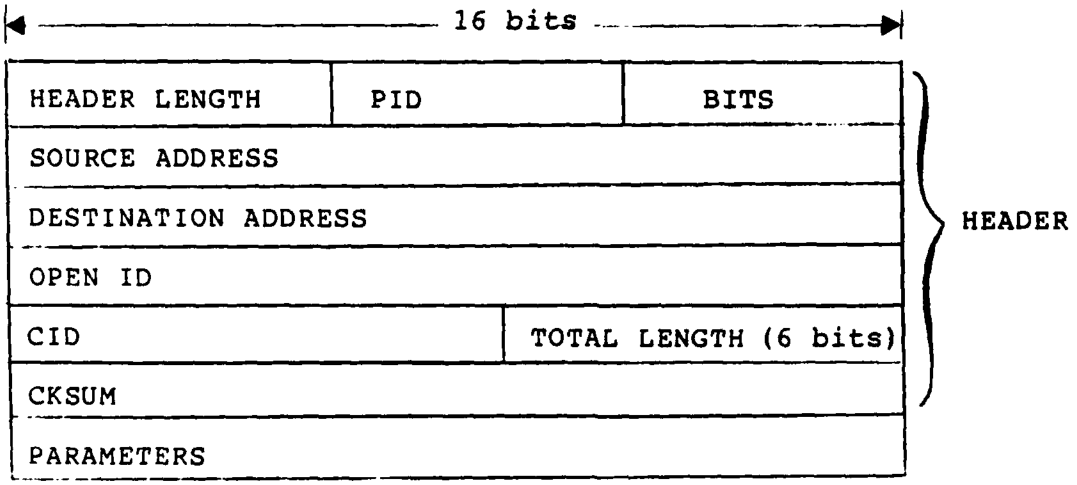
5. Receive output voice buffer to smooth variable packet delays and out of sequence packets
6. Transmit input voice buffer for voice packets with the time stamps and sequence numbers
7. Received voice packets (in talkspurts) disassembly to support speech reconstitution in the STU-IIs
8. Speech playout algorithms, if any used
9. Cryptosynchronization.

Several parameters were analyzed before deciding on the voice packet size.

First, to minimize packet delay and the deleterious effect of lost packets on voice quality, the size should be as small as possible. On the other hand, efficient digital voice transport in the DDN I will require that the number of speech bits in voice packets be as large as possible relative to the headers. The X.25 maximum user data size, default value of 128 octets, is the size limitation on a voice packet. This is smaller than the standard IP datagram length of 576 octets which all IP networks and hosts must support. Therefore if the selected voice packet size is less than 128 octets (for speech data), we will assure that all networks and future networks in the DDN will be able to transport the voice packets.

Secondly, our choice of input buffer and voice packet size were influenced by the typical range of the packet size used by C.J. Weinstein and J.W. Forgie with their real-time speech transmission experiments across the ARPANET [Reference (22)]. Based on the results in the paper it was decided to assemble five voice frames into a voice packet, realizing that experiments with the STU-IIs need to be conducted in future to obtain the optimum packet size. The 54-bit voice frames in talkspurts from the calling STU-IIs are received at the originating server every 22.5 milliseconds. Thus, an input buffer of 270 bits is required to techniques need be used with these packets. Only the control messages will be checked to ensure the correct connection setup. The NVP/ST headers will have to provide IP with all the information necessary for the successful delivery of the packets. The header will also have information independent of the ST agents, providing identification services to the destination host.

The NVP/ST will employ two types of packets, control and data, respectively for control and data messages. The control messages are sent from an ST agent to an ST agent as datagram packets with the ST agent identifier (CID) set to zero. The header will contain a BITS flag to identify the packet type. They will be allocated resources only when spare capacity exists. The control messages require an acknowledgement for a request. Control messages that are lost or ignored are retransmitted after a timeout. A packet may contain more than one control message, but a message will not extend beyond a packet boundary. The control message will have the format as shown in Illustration C-10.



16 bits

HEADER LENGTH	PID	BITS
SOURCE ADDRESS		
DESTINATION ADDRESS		
OPEN ID		
CID	TOTAL LENGTH (6 bits)	
CKSUM		
PARAMETERS		

Illustration C-10. NVP/ST Control Message Format

HEADER LENGTH: Total Length of Header

PID: Protocol Identification and Message Type

BITS: Bits specify if it is a control, point-to-point (PTP), or conference packet as follows:

00 = control
01 = PTP
11 = conference

SOURCE ADDRESS: Originator

DESTINATION ADDRESS: Recipient

OPEN ID: Identifies the source/destination link

CID: Is an arbitrary identifier assigned by the ST agent receiving the packet for the purpose of identifying the connection on which the packet is travelling. CID is unique to the agent that assigns it, and will change on each hop. Two nodes, at the least are cognizant of each CID.

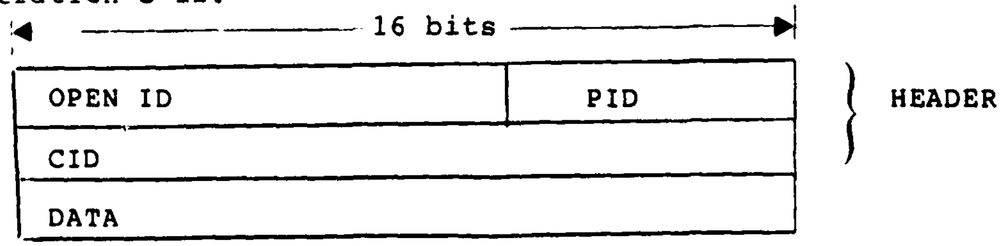
TOTAL LENGTH: Variable number includes header and parameters

CKSUM: Checksum used with the control messages.

PARAMETERS: parameters are sent as required for the particular PID/BITS combination. Each parameter is identified with a P-code byte, followed by a P-length byte indicating the length the parameter in words (16 bits) (It includes length of both P-code and P-length).

Control op-codes and parameters will change from conference to PTP connections, except for a few common ones; for example: [ACK], [HELLO],.....

The PTP NVP/ST data packet (message) has the format shown in Illustration C-11.



OPEN ID	PID
CID	
DATA	

Illustration C-11. NVP/ST Data Message Format

OPEN ID: As defined previously this ID is assigned to the connection after it is established. It is the same OPEN ID as in all the previous protocol headers.

CID: ST Agent Link Identifier

DATA: Contains all previous protocol headers and digitized voice.

C.2.4.3 NVP/ST Interfaces

The NVP/ST interfaces with both the IP and the VSP.

The VSP will call on the NVP/ST for a connection setup. The VSP will specify the address for the connection and the necessary parameters to the NVP/ST. The NVP/ST will then start its connection setup procedure. All NVP/ST messages including [open] request for connection setup, will use the IP for transfer through the network. Therefore, the NVP/ST will call on the IP, specify all the necessary parameters, and send its control message as the data part of the IP message format.

The NVP/ST counterpart at the destination node is called by the IP that passes to it the control message containing [open] request. The destination NVP/ST responds to the open request sending back the new open identification number stored in the control message header as a positive acknowledgment of an established connection.

At the source NVP/ST once the acknowledgment is received, as a response to the [open] request, a return to the VSP passing the just received OPEN ID, will be done.

C.2.5 The Internet Protocol (IP)

The IP is used in the CATENET environment of packet-switched networks to provide for the transmission of blocks of data from source hosts to destination hosts. The IP sits on top of the network layer and will be used in the DDN for data transport and all host implementations will be required to support it. See Reference (7) for details on functions and services, message formats, and interfaces of the DoD standard IP, which was employed in our protocol architecture.

C.2.6 Voice DDN Network Access Protocol

A basic requirement for the Voice Interface Processor (VIP) is to access the DDN using the DDN X.25 standard interface protocol [Reference (6)]. The VIP interface to the DDN must support the exchange of X.25 packets between the VIU and the DDN PS node. See the reference for details on the functions and services, message formats, and interfaces of the DoD standard X.25 interface, which was employed in our protocol architecture.

C.3 PROTOCOL IMPLEMENTATION CONSIDERATIONS

The protocol architecture will be implemented in external processor(s) and/or the DDN Terminal Access Controller (TAC) of the VIU. One alternative is to incorporate the proposed protocols in the DDN TAC. Another alternative is to use external processor(s). Additional protocol architecture implementation alternatives will result from using the combination of TAC and/or external processors.

Another major protocol architecture implementation consideration is the incorporation of the ST agents in the DDN PS nodes and gateways. Modifications will have to be introduced into the DDN switch (DDN PS nodes and gateways) software to implement the ST agents. These agent's primary function, when introduced, is to translate the NVP/ST header and to assist in the management and routing of the voice packets. In the present case, ST agents are not available in the DDN switch software. Therefore, a temporary alternative is given. Results of experiments conducted on existing packet-switching networks show that under normal or light network load, the packet route established between two users is seldom modified, with packets arriving at its destination in a sequential order with normal delay [References (22) and (23)]. However, with heavy network load, packets will adopt different routes, and delays and out-of-sequence delivery is possible. In this case, a certain degradation of the system performance for voice would be expected. The case in which the ST agents are introduced in the DDN switches, is essential for the guaranteed delays and sequential arrivals of voice packets. These two cases are discussed in detail in Paragraph C.2.4.1.

The cost estimate for implementing the proposed protocol architecture software is shown in Illustration C-12. This is based on defining the functions necessary to implement the protocol architecture and the subdivision of functions to subfunctions which can be coded with less than 100 lines of code. Illustration C-13 shows the cost of selected processors which are candidates for external processors.

C.4 SCENARIOS

In this paragraph, we explain how the proposed implementation protocol architecture supports the following scenarios:

1. Call initiation and termination
2. Point-to-point connection setup
3. Voice packet transport.

This will be achieved by employing the two-part (DVS and DVT) functional view of the proposed implementation protocol architecture and the protocol components of these functional parts (Illustration C-14). The DVS and DVT will physically reside in the Processor Module of the VIUs (Illustration C-15) which indicates how the STU-IIs can be interfaced through the VIUs to the DDN I.

PROTOCOLS ▶	VAP	VPP	VSP	NVP/ST	IP	PS NODE	GWY	TOTAL	$ TOTAL
						(ST Agents)			
LOC (with ST)	800	400	120	800	-	400	400	2920	$280,758**
No. Weeks (with ST)	20	10	3	20	-	10	10	73	
LOC (no ST)	1200*	400	120	800	-	-	-	2520	$242,298**
No. Weeks (no ST)	30	10	3	20	-	-	-	63	

Assumptions: 1. 40 lines/week/programmer

2. $\$/\text{week/programmer} = \frac{100,000}{52} = 1,923$

Notes: 1. LOC = Lines of Code

2. * It is estimated that LOCs for the VAP (without ST) will be 50% higher than those for the VAP (with ST) because it has to implement ST like functions in it to ensure an acceptable voice capability when ST agents are not used in the DDN I switching nodes.

3. ** An additional software engineer is considered for the entire duration of the software development to participate in requirements, design, testing, and specifications.

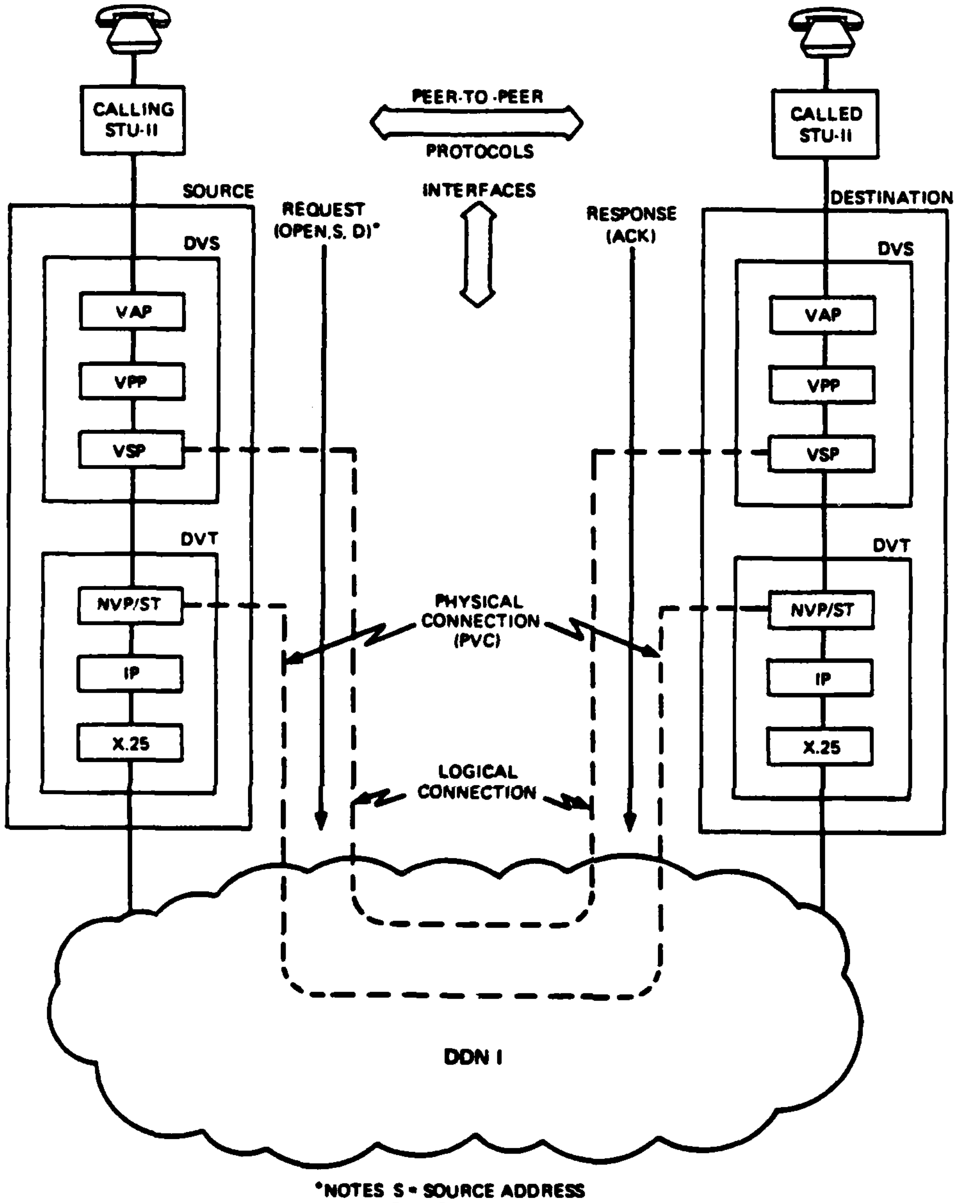
Illustration C-12. Cost for Implementing the Protocol Architecture Software

ITEM NO	VENDOR	MODEL	PRICE
1	ALTOS COMPUTER	ACS 586-10	7,990
2	FORTUNE SYSTEMS CEPR.	FUTURE 32:16	5,000 - 20,000
3	INSTRUMENTATION LABORATORY	PIXEL 1001 AP	15,000
4	NCR CORP.	TOWER 1632	11,785
5	APPLIED SYSTEM CORP	ASC 8026 18028	4,000
6	DATA GENERAL CORP	DESKTOP GENERATION MODE 10	5,430
7	GOULD SEL	PS 100	7,000 - 10,000
8	BBN	C/30	25,000
9	BURROUGHS CORP	CP9582	27,000
10	CONTROL DATA	MODE L 2551-1	50,000

Note: Assumed Processor Price (used in the Processor Module of the VIU) = $22,000

(For implementation involving the TACs, the processor price = 0 since the TAC is assumed available at the sites)

Illustration C-13. Hardware Cost for Candidate External Processors



*NOTES S = SOURCE ADDRESS
D = DESTINATION ADDRESS
PVC = PERMANENT VIRTUAL CIRCUIT

TP No. 026-16261-A

Illustration C-14. Message Flow Supporting the Scenarios

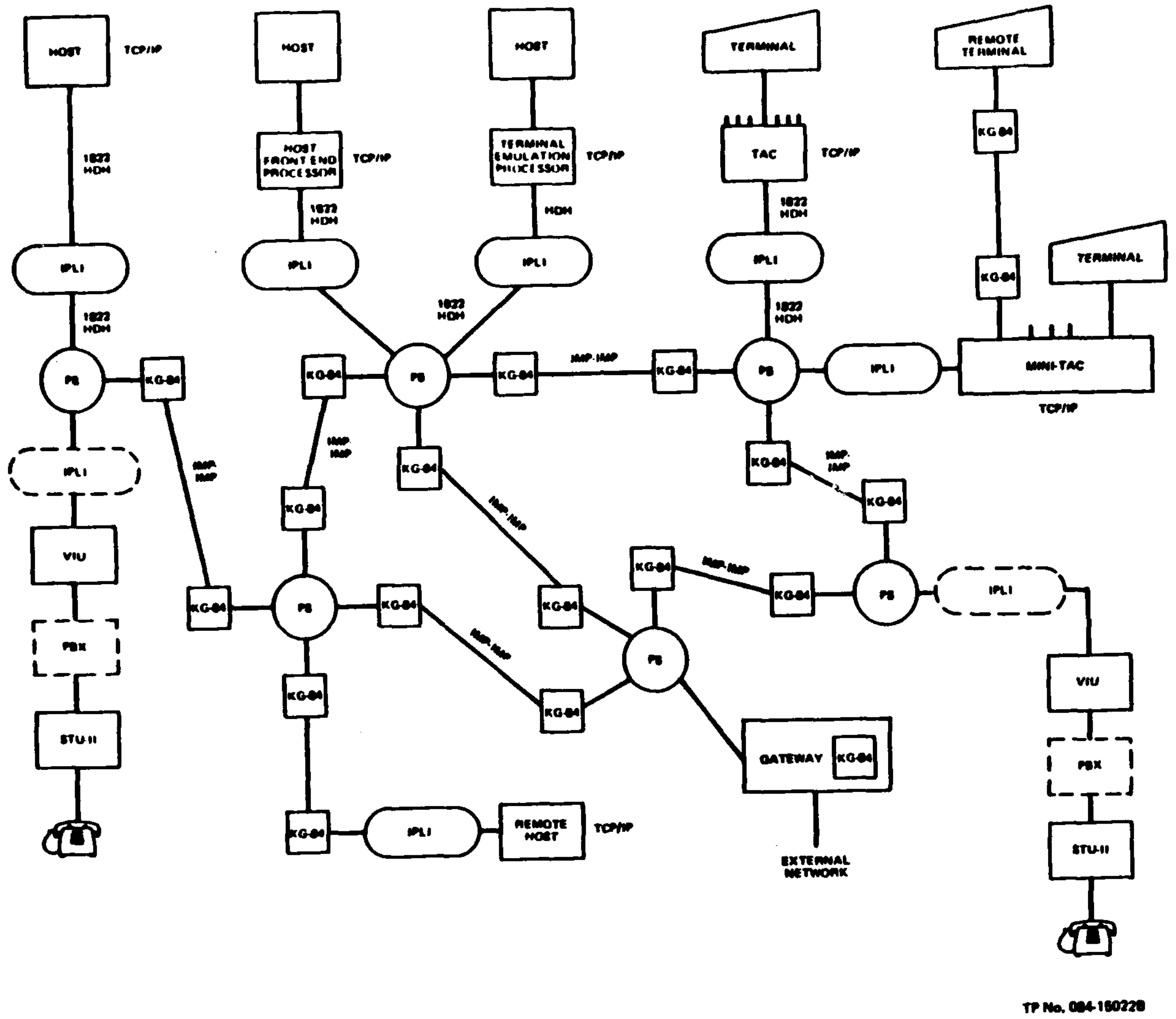


Illustration C-15. Simplified Architecture of the DDN I Incorporating the STU-IIs

The source DVS is driven by signals and messages (control and voice) from the calling (source) STU-II. The OFF-HOOK signal from the calling STU-II initiates the digital telephone connection by activating the VAP, the first protocol in the source DVS. The source VAP is placed in the wait state until the number of the called party is dialed in using either the Dial pulse or DTMF signals. The source VAP will then translate the dialed number to a proper network address of the called STU-II, by looking up the corresponding number in a table. The source VAP will use this address to initiate the call.

The source VAP will initiate the call with an [open] command, specifying source and destination addresses. The source VAP interface will call on the source VPP to start the open process. The call will include the source and destination addresses and an open command. The source VAP open message will wait for a connection. The source VPP will take that call, prepare its own open command, and call on the source VSP to continue the open process. This is achieved by the source VPP interface calling the source VSP and specifying the open and address parameters. The source VPP will then wait with its open message for a connection. The source VSP interface will call the source DVT to open a connection for the transport of all the waiting messages.

The source DVT starts by activating the source NVP/ST. The source and destination address and the open command are issued in the source VSP call to the source NVP/ST which will proceed to open a point-to-point connection between the calling and called (destination) STU-IIs. The source NVP/ST will prepare its connect message, and call on the IP for transport. This call will include the addresses. The IP will use the X.25 for interfacing and sending the message into the DDN I network. If the ST agents are not present in the DDN I, the IP will transport the message as a datagram to the destination NVP/ST. If the ST agents are present, then these agents will establish a connection [a permanent virtual circuit (PVC) fixed route] between the source and destination NVP/ST hosts. The message can then be sent over this PVC fixed route. The message, received at the destination IP layer, will be stripped of the IP header and sent to the destination NVP/ST. The destination NVP/ST will then prepare a response, an acknowledgement, or a refuse with reasons. A refuse will cause a termination of the connection, and is discussed later in the paragraph.

When the source NVP/ST receives an acknowledgement, the connection is established. At that time an open identification (ID) for the connection will be generated from a central process and assigned to the STU-II pair to be connected. The source NVP/ST is now ready to send data messages (voice packets) to the destination NVP/ST. All the higher level control messages will be considered data by the NVP/ST. The NVP/ST data message header will contain the assigned open ID, to identify all voice packets transfered between that pair of STU-IIs. The peer DVT connection is now finalized and an acknowledgement is sent back to the originating DVS to start its own connection setup procedures.

The VSP in the originating DVS, upon receiving the connection acknowledgement containing open ID from the destination DVT, will send its waiting open command over the established source-to-destination DVT PVC connection (when ST agents are present), to setup a logical connection with its peer protocol at the destination DVS. The destination VSP will send either an acknowledgement or a refusal back to the source VSP. A refusal will result in termination. Acknowledgement will result in the source VSP sending the acknowledgement to the source VPP with the open ID. The source VSP is now ready to send data messages, containing the higher level messages, to its peer protocol at the destination over the established connection. The open ID is part of its data message header, and is used to identify different users in a multiuser connection, and for data management.

The source VPP can now send its control messages as VSP data message, and conduct negotiations with its peer protocol (VPP) at the destination to determine the maximum set of mutually acceptable characteristics of the STU-IIs. If compatibility is achieved, the destination VPP will acknowledge the connection. The source VPP, upon receiving the acknowledgement, will send it along with the open ID, to the source VAP. The peer VPPs are now ready to exchange data messages. The source VAP will then issue its waiting open command to complete the connection with destination VAP. The destination VAP will respond to this command, with either a ready or a not ready response (with reasons). When the destination VAP is ready, it will send a ringing signal to its STU-II, and a ready response to the source VAP. Upon receiving this response, the source VAP will send a ringing tone its STU-II. If the destination VAP is not ready, the source VAP will send a busy signal to its STU-II. When the "ringing" STU-II (called STU-II) goes OFF-HOOK, the ringing signal is halted and the destination VAP sends a "stop ringing" message back to the source VAP and its STU-II. This completes the call initiation and point-to-point connection setup. The system is now ready for full-duplex voice message transport as described in Paragraph C.2.

Termination of the connection will result from either a malfunction or normally from an ON-HOOK signal from a STU-II. A malfunction could happen anywhere in the component protocols of the DVT and DVS, at any time during and after the call initiation. A fatal communications fault would terminate the connection at the NVP/ST level. A wrong address would not receive an acknowledgement by the NVP/ST. If no responses are received for a command in any protocol level above the NVP/ST, the connection will be terminated. Voice performance problems, such as large end-to-end delays or loss of excessive voice packets will be detected in the VAP and result in a termination.

When a termination occurs a disconnect message is transparently passed on to the VAP level without affecting the intermediate levels. The VAP, upon receiving the disconnect, will send it to its STU-II through the S/S module which will generate a dial tone that indicates that the connection has been terminated. The VAP will then issue a disconnect message which will transfer down the levels. Each successive layer protocol will disconnect its connection with the peer protocol before sending the disconnect to the lower level. The termination will end at the NVP/ST level. Once terminated the caller will have to place his call again.

The call initiation, connection setup, and call termination related control commands (including STU-II control messages) are executed in the clear. After the connection is established, the GO SECURE request can be issued for encrypted voice sessions. When this happens, the same number of bits sent by the calling STU-II must be received by the called STU-II to maintain cryptosynchronization. This is enforced by the VAP at the called STU-II.

When the STU-II call precedence bits are used the call will be able to get through with highest priority; the type of priority and related procedural changes in the DDN I will have to be worked out during a formal specification of the protocol architecture.

C.5 SUMMARY

In this Appendix an implementation protocol architecture to support secure digital voice in the DDN is proposed. It satisfies the requirements of the DDN of 1980s time-frame (DDN I) and yet is

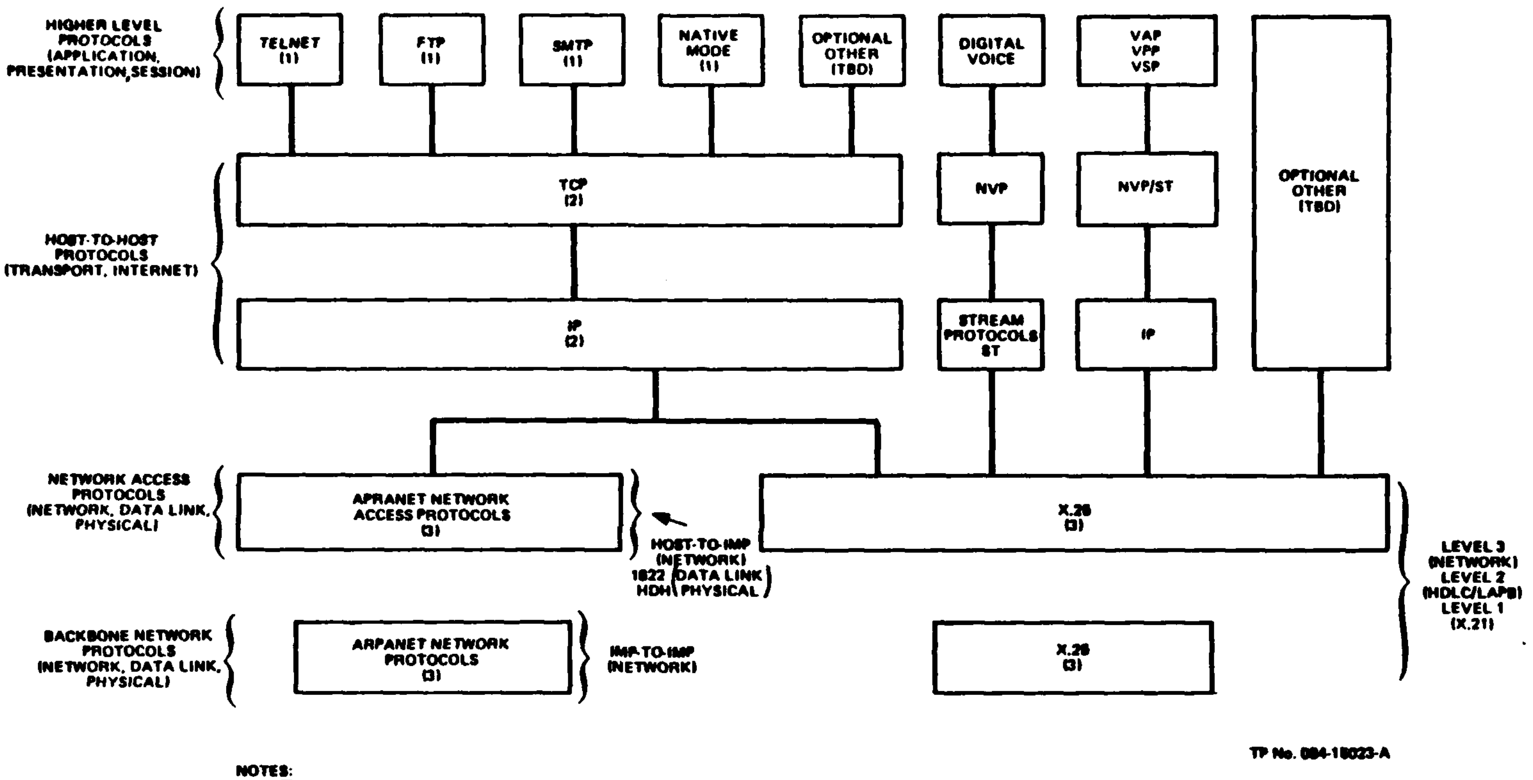
.exible enough to satisfy the expanded requirements of the DDN of '90s time-frame (DDN II). This is accomplished by using :andardized network access (X.25) and transport (IP) protocols .th a special NVP/ST protocol based on the ST protocol. Iditional higher level protocols (VAP, VPP, and VSP) are defined ;ing many aspects of the NVP to support higher level functions.

Illustration C-16 indicates how the proposed model of the :otocol architecture fits in with the DDN I planned protocol rchitecture. See Appendix B for a high level description of the)N I planned protocol architecture.

Illustration C-17 shows the message format that will be used ɔ transport the voice packets through the DDN I. Illustration -18 depicts the details of the overhead employed in the message ɔrmat for various layers in the proposed protocol architecture or control and data (containing voice packets) messages. llustration C-19 summarizes the overhead bits used in each ayer. From this illustration it is clear that the shorter onnection setup message (marked by x) will be 352 bits long (with 36 bits of overhead) and the data message (marked by*) containing voice packet (or five voice frames) will be 574 bits long (with 04 bits of overhead).

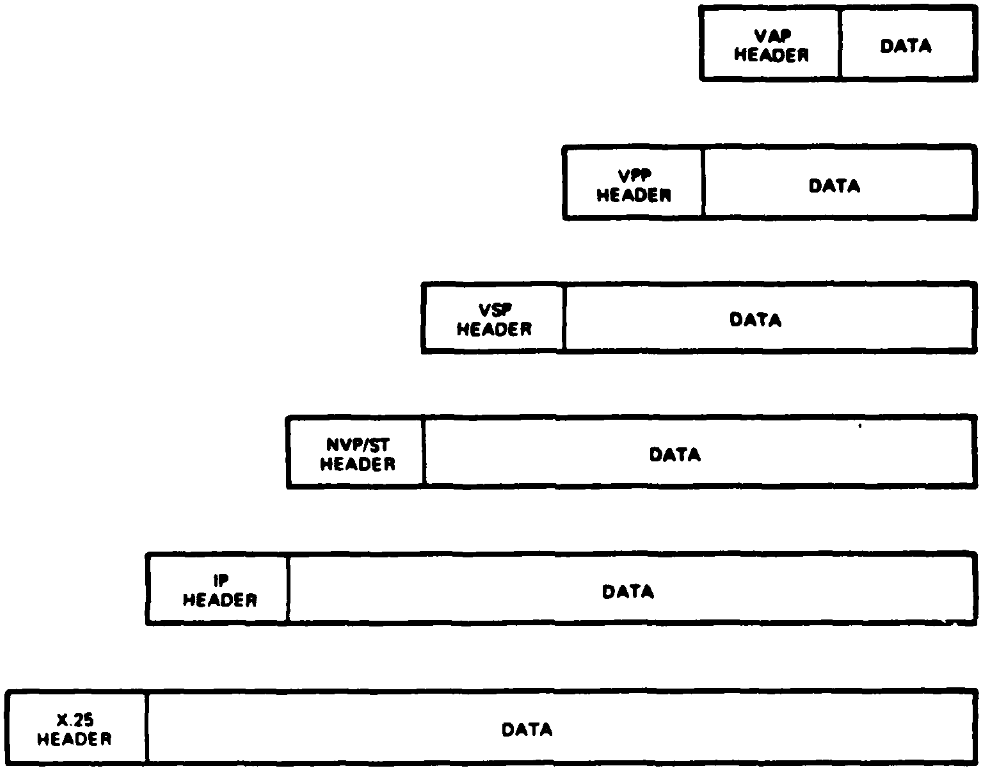
The cost of implementing the proposed protocol architecture s provided. It is made up of hardware cost and software cost. ardware may include TAC and or external processor in the rocessor module of the VIU, with TAC assumed available at no cost nd $22,000 as the cost per external processor used. Software ost with ST agents is roughly $281K and without ST agents, oughly $242K.

Protocol support for typical call initiation, point-to-point onnection setup, voice packet transmission, and call termination cenarios is described.


HIGHER LEVEL PROTOCOLS (APPLICATION, PRESENTATION, SESSION)
TELNET (1)
FTP (1)
SMTP (1)
NATIVE MODE (1)
OPTIONAL OTHER (TBD)
DIGITAL VOICE
VAP VPP VSP
OPTIONAL OTHER (TBD)
HOST-TO-HOST PROTOCOLS (TRANSPORT, INTERNET)
TCP (2)
NVP
NVP/ST
IP (2)
STREAM PROTOCOLS ST
IP
NETWORK ACCESS PROTOCOLS (NETWORK, DATA LINK, PHYSICAL)
APRANET NETWORK ACCESS PROTOCOLS (3)
HOST-TO-IMP (NETWORK) 1822 (DATA LINK HDH (PHYSICAL
X.25 (3)
LEVEL 3 (NETWORK) LEVEL 2 (HDLC/LAPB) LEVEL 1 (X.21)
BACKBONE NETWORK PROTOCOLS (NETWORK, DATA LINK, PHYSICAL)
ARPANET NETWORK PROTOCOLS (3)
IMP-TO-IMP (NETWORK)
X.25 (3)
TP No. 084-18023-A

NOTES:
(1) RECOMMENDED FOR DDN HOSTS
(2) MANDATORY FOR DDN HOSTS
(3) ONE OF THESE IS MANDATORY

Illustration C-16. DDN I Planned Protocol Architecture with the Proposed Protocol Architecture for Secure Digital Voice



TP No. 025-16638-A

Illustration C-17. Message Format Used for the Transmission of Voice Packets in the DDN I

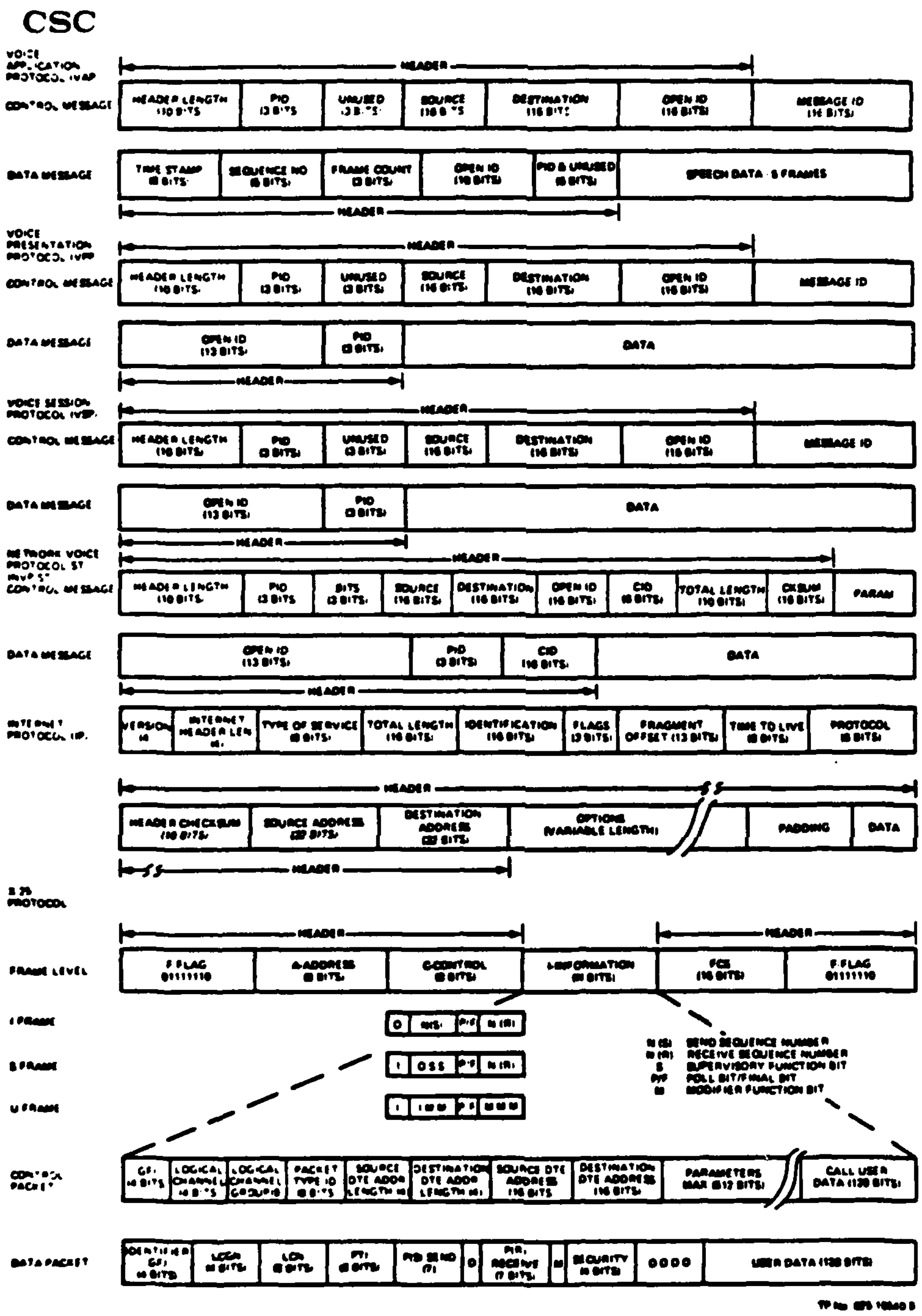


Illustration C-18. Detailed Overhead Format Used in the Layers of the Proposed Protocol Architecture

PROTOCOL	NUMBER OF BITS		EFFECTIVENESS (DATA/TOTAL LENGTH PER PROTOCOL)
	HEADER	DATA	
VAP CONTROL MESSAGE DATA MESSAGE	 64 (X) 32 (*)	 16 (X) 270 (*)	 20% 89%
VPP CONTROL MESSAGE DATA MESSAGE	 64 16 (X) (*)	 16 80 – 302	 20% 83% TO 95%
VSP CONTROL MESSAGE DATA MESSAGE	 64 16 (X) (*)	 16 80 – 318	 20% 83% TO 95%
NVP/ST CONTROL MESSAGE DATA MESSAGE	 96 32 (X) (*)	 16 80 – 334	 14% 71% TO 91%
IP (DATA MESSAGE)	160 (X) (*)	112 – 366	41% TO 70%
X.25 (DATA MESSAGE)	48 (X) (*)	272 – 526	85% TO 92%
TOTAL			
* (DATA MESSAGE)	304	270	47%
X (CONNECTION SETUP MESSAGE)	336	16	5%

TP No. 028-16537-A

Illustration C-19. Overhead and Data bits Used by the Message in the Proposed Protocol Architecture

REFERENCES (1 of 2)

1. "Worldwide Digital System Architecture, Final Report;" (DCEC); December 1981.

2. "Secure Digital Voice Communications in the Defense Data Network (DDN) (U) (Draft);" Computer Sciences Corporation (CSC); August 1984.

3. "Department of Defense Automated Data System Documentation Standards;" DoD Standard 7935.1-S; 13 September 1977.

4. "Interface Message Processor, Report No. 1822;" BBN; December 1981 Revision.

5. "Recommendation X.25: Interface between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) for Terminals Operating in the Packet Mode on Public Data Networks;" International Telegraph and Telephone Consultative Committee (CCITT).

6. "Defense Data Network X.25 Host Interface Specification;" DCA; December 1983.

7. "Military Standard on Internet Protocol;" MIL-STD-1777.

8. "Military Standard on Transmission Control Protocol;" MIL-STD-1778.

9. "Military Standard on TELNET Protocol and Options;" MIL-STD-1780.

10. "Military Standard on File Transfer Protocol;" MIL-STD-1780.

11. "Military Standard on Simplified Mail Transfer Protocol;" MIL-STD-1781.

12. "Specifications for the Network Voice Protocol (NVP);" Network Information Center (NIC) (at SRI International); 22 November 1977.

13. "ST-A Proposed Internet Stream Protocol;" J. Forgie, MIT Lincoln Laboratory; 7 September 1979.

14. DoD Protocol Reference Model, TM-7172/201/04;" System Development Corporation (SDC); 2 December 1983.

REFERENCES (2 of 2)

15. "Defense Data Network Program Plan;" DCA, May 1982 Revision.

16. "Defense Data Network System Description;" MITRE Corporation January 1984.

17. "SVIP/SVGC Integration Functional System Design, Final Report (U); GTE (CSD); 11 November 1982; CONFIDENTIAL

18. "In-House Discussions at Computer Sciences Corporation (CSC) on STU-IIs;" CSC Personnel involved with SVIP; July-August 1984.

19. "SVIP Program Interface Specification Documents (U);" ITT (DCD); SECRET and CONFIDENTIAL.

20. "Trip Report - ITT Nutley, NJ;" Walter Drum of DCEC (Code 630); 30 May 1984.

21. "Reference Model of Open Systems Architecture (Version 3) ISO/TC97/SC16 N117;" Also published as INWG Note 188 and ANSI X3537-78-176.

22. "Experience with Speech Communication in Packet Networks;" IEEE Journal on Selected Areas In Communications C.J. Weinstein and J.W. Forgie; December 1983.

23. "Conference meeting with Gary Toess of BBN regarding BBN switch capabilities in dynamic routing (held at CSC);" December 1984.

END

FILMED

7-85

DTIC